

# 5 Schritte zu mehr IT-Sicherheit

## Schritt 1 | IT-Inventarisierung

Scannen Sie dauerhaft Ihre IT-Umgebung nach vorhandenen Geräten und schaffen Sie ein Live-Abbild Ihrer IT-Infrastruktur.

Automatische Erkennung und unbegrenzte IP-Inventarisierung aller Netzwerkgeräte, sowie deren Klassifizierung.

- Live Inventar
- Monitoring aller erkannten Geräte
- Erfüllung der IP-Inventarisierung nach ISO-27001

## Schritt 2 | IT-Security Analyse von innen

Unser SaaS liefert eine umfassende Lösung zur Überwachung und Absicherung Ihrer Windows-Server, Linux-Server und Endgeräten, wie Windows-PC oder Linux-PC.

Sie erhalten eine komplette Übersicht Ihrer gesamten IT.

- 100% validierte Erkennung von Sicherheitslücken (CVE-Scan)
- Best Practise Security-Konfigurationen erkennen und einspielen
- Live-Erkennung und Verhaltensanalyse von Netzwerk-Angriffen (Intrusion Detection System)
- Alarmierung bei unberechtigten Zugriffen

## Schritt 3 | IT-Security Analyse von außen

Webanwendungen, wie bspw- Webseiten, überwachen wir hinsichtlich Verfügbarkeit und Sicherheit.

Lassen Sie keine Schlupflöcher in Ihren Webanwendungen unbemerkt und schützen Sie sich, Ihre Daten sowie die Besucher Ihrer Webseite vor Cyber-Kriminellen.

- Erkennung von Sicherheitslücken in Ihrer Webanwendung und auf Ihrem Webserver
- Web-Monitoring / Port-Monitoring
- Handlungsempfehlungen zu sicherheitsrelevanten Konfigurationen
- Zertifikate-Management

## Schritt 4 | Security-Prozesse automatisieren

Mit unserem Security as a Service können wir auf Systemereignisse automatisch reagieren und Routineaufgaben autonom ausführen lassen.

Nutzen Sie unsere vielfältige Automatisierungsmöglichkeiten und geben Sie Ihrer IT-Abteilung wieder Luft zum Atmen.

- Automatisierte Handlungen im Alarmfall
- Autofix von Sicherheits-Konfigurationen
- Workflows automatisieren
- Automatisches Patch-Management
- Zeitersparnis: 30 bis 50 %

## Schritt 5 | Automatisierter Penetrationstest

Mithilfe unseres automatisierten Penetrationstests können Sie Ihre Systeme regelmäßig auditieren und mögliche Einfallstore für Hacker frühzeitig erkennen.

- Durchführung spezifischer Angriffs-Szenarien z.B. Bruteforce-Attacken
- Automatischer Security-Audit für Server, Clients, Webseiten und ganze Netzwerksegmente
- Zusätzlicher Schwachstellen-Scan
- Ausführliches Reporting

Gerne unterstützen wir Sie bei der Umsetzung!



[www.2consulting.eu/saas](http://www.2consulting.eu/saas)



[hello@2consulting.eu](mailto:hello@2consulting.eu)



+49 (0) 89 - 904 227 390