



CASE  
STUDY

# Schwachstellen- Management leicht gemacht

# 1.000.000 Sicherheits probleme mit nur 80 Workouts beheben

Unter IT-Mitarbeitern bekannt und gefürchtet: Überforderung durch Unmengen plötzlich auftretender Cyber Security Probleme. Die Schwachstellen sind entdeckt, doch welche müssen zuerst behandelt werden? Und wie? Lesen Sie in dieser kurzen Fallstudie, wie ein Kunde 1.000.000 Sicherheitslücken – entdeckt durch Online Security Scanner wie Qualys, Nessus oder Rapid7 – durch nur 80 unserer Workouts beheben konnte. 80 benutzerfreundliche, einfach durchführbare und von Experten empfohlene Prozesse, die Unternehmen für das erfolgreiche Schwachstellen-Management brauchen. Erfahren Sie in einem kostenlosen Expertengespräch, wie wir Ihre individuellen Herausforderungen bewerten und Sie mehr Cyber-Sicherheit führen!



## Über Autobahn Security

Autobahn Security ist eine SaaS-Plattform, die IT-Sicherheitsexperten Zeit spart und IT-Teams in die Lage versetzt, ihre Netzwerke sicherer zu machen. Unsere Plattform aggregiert, filtert und priorisiert Schwachstellen aus verschiedenen Scannern und verwandelt sie in leicht verständliche Lösungsempfehlungen. Autobahn Security ist das Ergebnis jahrzehntelanger Erfahrung im White-Hat-Hacking und in der Sicherheitsberatung für Fortune-500-Unternehmen. Autobahn genießt das Vertrauen von Unternehmen aus unterschiedlichen Branchen in über 20 Ländern, darunter Allianz, SwissPost und Taboola.

# Das Problem: Überforderung des IT-Teams durch 1 Million Cyber Sicherheits- probleme

Der Vorfall begann mit einer routinemäßigen Schwachstellen-Analyse. Unser Kunde – ein namhafter Softwarehersteller – verwendete einen bekannten Online Security Scanner, um Sicherheitslücken im internen und externen Produktionsnetzwerk zu erkennen.

Als plötzlich eine Sturzflut von Problemen zu Tage trat, fühlte sich das IT-Sicherheitsteam des Unternehmens überwältigt. Wer fiel nicht in Ohnmacht angesichts fast einer Million Probleme? Das Ausmaß an Zeitaufwand und gebundenen Expertenressourcen, das nötig würde, um schnell wirksame Abhilfe zu schaffen, ließ die Mitarbeiter fast erstarren.



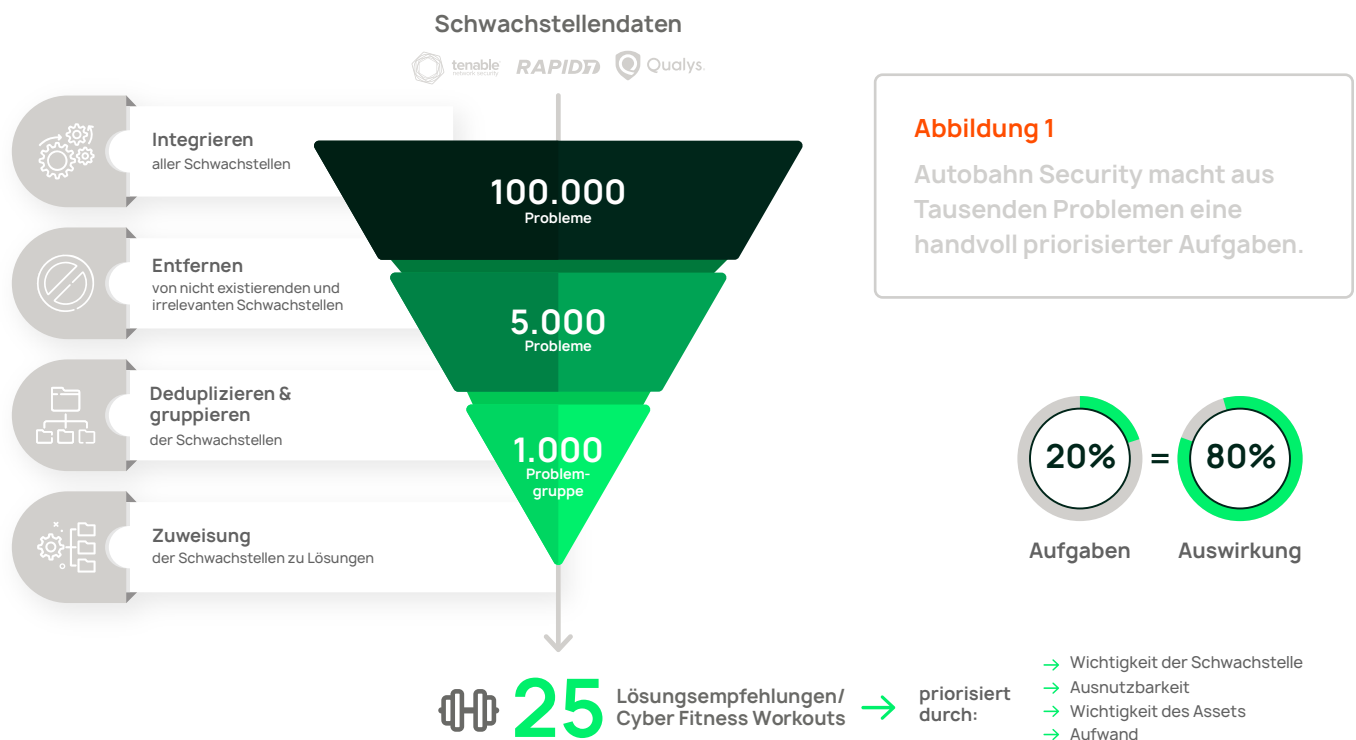
**Die Lösung:**  
Gruppierung und  
Priorisierung, um  
Sicherheitsprob-  
leme schrittweise,  
effektiv und schnell  
zu neutralisieren

Nur 3 Probleme  
bedeuteten 50%  
Hackability für das  
Unternehmen

Das Cyber Security Team des Unternehmens brauchte umgehend eine praktikable Lösung. Was, wenn es eine Möglichkeit gäbe, um 1 Million Probleme nach Art und Dringlichkeit zu ordnen und dann schrittweise zu beheben? Das Team begann mit der Suche nach Software-Tools und SaaS-Plattformen, die genau dies leisten würden.

Schließlich kam Autobahn Security zum Einsatz! Schnell wurden Workouts identifiziert, die die Produktionsnetzwerke unseres Kunden effektiv beeinflussten. Es stellte sich heraus, dass nur 2 Workouts in 2 Produktionsnetzwerken über 40 % der gesamten Hackability Probleme des Unternehmens lösten!

Durch den internen Scan konnte Autobahn Security schon bald 720 Produktionsumgebungen mit kritischen bis schwerwiegenden Problemen identifizieren. Das Gesamtbild aller gefundenen Ereignisse verdeutlichte: aus der Vielzahl von internen Schwachstellen waren es gerade einmal 3, die für eine Hackability von 50% sorgten, vornehmlich durch Red Hat Linux Patching Probleme im internen Netzwerk. Und auch der externe Scan brachte ermutigende Ergebnisse: durch die Anwendung eines Autobahn Workouts zum Patchen einer Webserver-Implementierung in einem extern erreichbaren Netzwerk konnte der Kunde über 15 % der externen Schwachstellen beheben.



# Konfrontiert mit Schwierigkeiten bei der Bewertung und Priorisierung von Cyber Sicherheitsproblemen in Ihrem Unternehmen?

Sie möchten herausfinden, wie auch IT-Spezialisten ohne Security Expertise Sicherheitslücken beheben können? Vereinbaren Sie jetzt ein kostenloses Expertengespräch vereinbaren

[Sprechen Sie mit uns →](#)

Lassen Sie Hunderttausende von Schwachstellen, aufgedeckt durch renommierte Scanner wie Qualys, Nessus, Rapid7 und andere, einfach durch den Aggregations- und Priorisierungs-Filter von Autobahn laufen, um ganze Ozeane von Problemen in eine benutzerfreundliche, leicht zu befolgende und von Experten empfohlene Essenz von Workouts zu verwandeln.

# Wie Ihr IT-Team priorisierte Lösungen einfach anwenden kann

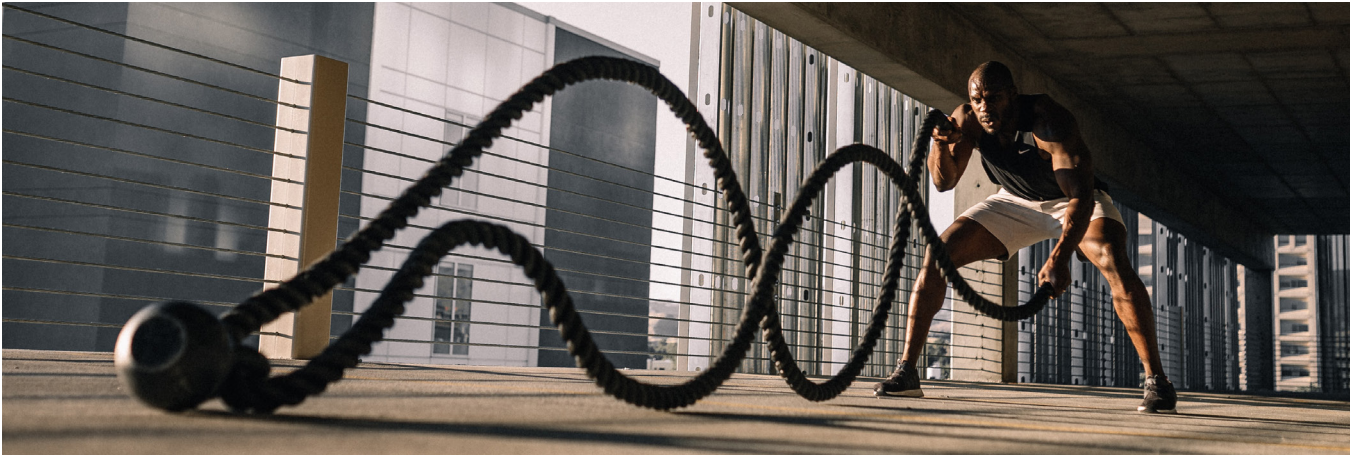
Die Möglichkeit alleine, die IT-Assets Ihres Unternehmens zu scannen und Sicherheitsrisiken zu identifizieren, macht Ihr Unternehmen noch nicht sicher. Eine erfolgreiche Problemlösung hängt von einem Priorisierungsplan ab, der die Auswirkungen der Probleme sowie deren Lösung auf die Sicherheitslage Ihres Unternehmens zu berücksichtigen vermag. Identifizierte Risiken müssen zuerst nach ihrer Kritikalität sortiert werden. Und genau hier kommen die Cyber Fitness Workouts von Autobahn Security zum Tragen.

The screenshot displays the Autobahn Security Cyber Fitness Workouts interface. The left sidebar shows the navigation menu with options like Cyber Fitness, Dashboard, Workouts, Scanning, Overview, All scans, Assets, Issues, and Team. The main content area is titled 'Patching NGINX' and includes a 'Warm up' tab. Three key metrics are shown: EFFORT (Medium), HACKABILITY SHARE (63.90% since 31 Jul 2022 00:00), and HOST(S) (3). Below these metrics, there is a description of NGINX, a risk assessment, and an objective for the workout.

## Abbildung 2

Beispiel für ein Cyber-Fitness-Workout auf der Autobahnplattform. Jedes Workout beschreibt den Aufwand und die Auswirkungen auf die Hackability Ihres Unternehmens, die nach der Ausführung des Workouts zu erwarten sind.





Selbst bei breiten Spektren von Hackerangriffen können Sie mit Autobahn mehrere Probleme gleichzeitig beheben, indem Sie einen einzigen Patch installieren oder einige wenige Einstellungen anpassen, um Ihr System zu härten. Die typischen Cyber Fitness Workouts von Autobahn Security erklären, wie genau das geht: Sie bestimmen, welche konkreten Schritte unternommen werden müssen, um Ihr Unternehmen sicherer zu machen.

Beispiel: ein Patch-Workout enthält meist einen Schritt, der zeigt, wo die letzte stabile Softwareversion lag. Zudem zeigt das Workout, welche Systemvoraussetzungen bei einem Update zu beachten sind oder wie man ein Backup durchführt. Darüber hinaus gibt das Workout Aufschluss darüber, wie Sie Updates automatisieren oder einige von ihnen zurücksetzen können, und es zeigt Ihnen, in welcher Reihenfolge bestimmte Komponenten aktualisiert werden müssen.

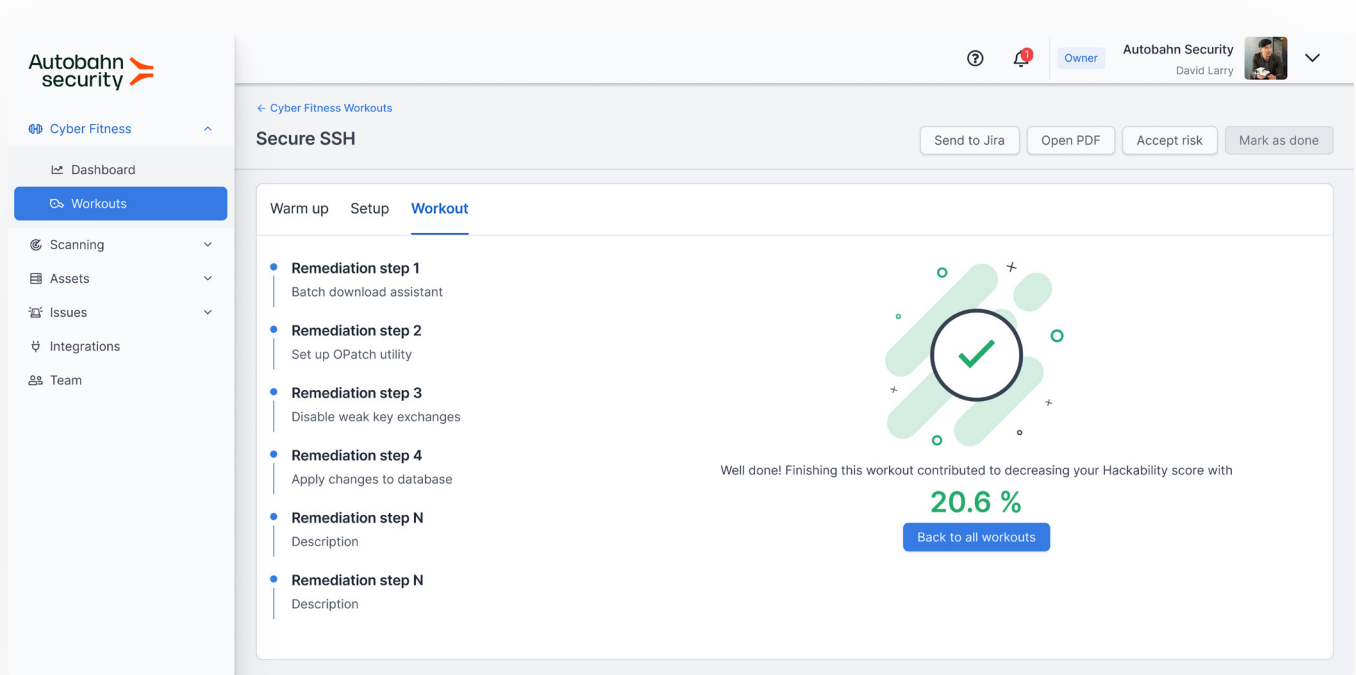
The screenshot shows the Autobahn Security platform interface. On the left is a sidebar with navigation options: Cyber Fitness, Dashboard, Workouts, Scanning, Assets, Issues, and Team. The main content area is titled 'Patching NGINX' and shows a list of remediation steps. The first step, 'Remediation step 1', is selected and expanded, showing an 'Initial recommendation' and a detailed description of the process. The description includes instructions on using stable versions and installing NGINX Open Source from a package. Navigation buttons for 'Previous' and 'Next' are visible.

### Abbildung 3

Beispiel für die Schritte eines Cyber-Fitness-Trainings auf der Autobahn-Plattform. Sie sind detailliert dargestellt und können auch von Nicht-IT-Sicherheitsexperten durchgeführt werden.

Ihr IT-Team wird begeistert sein: ausgestattet mit dem notwendigen Reparaturset müssen sie nur die Lösungen anwenden – und vielleicht ein Ticket an Jira senden, um den Fortschritt zu verfolgen.

Jedes Cyber-Fitness-Workout, das Sie absolvieren, verringert Ihren Hackability-Score und bringt Sie einer idealen Sicherheitshaltung näher.



**Abbildung 4**

Beispiel für ein abgeschlossenes Cyber Fitness Workout auf der Autobahn Plattform.





Wie Sie loslegen  
und was Sie  
innerhalb von nur  
1 Woche von uns  
erwarten können:

01. Verstehen Ihrer Problembereiche und des Problembehebungsprozesses
02. Einführung in die wichtigsten Aspekte der Plattform
03. Einrichten von Scans
04. Auswertung der Scan-Ergebnisse

Fordern Sie jetzt  
gleich ein  
kostenloses  
Expertengespräch  
an

Wir bewerten Ihre individuellen Herausforderungen und vereinbaren einen Demo-Termin mit Ihnen. Hier verschaffen wir Ihnen einen Überblick über unsere Prozesse und besprechen erreichbare Meilensteine und mögliche nächste Schritte.



Sprechen Sie mit unserem Team und erfahren Sie, wie Sie mit Autobahn Security cyber-fit werden.

Sprechen Sie mit uns —>