CASE STUDY

Wie ein DAX-Konzern mit 1 Millionen Schwachstellen umging

Inklusive Hilfestellung für eure ROI-Berechnung

Autobahn security

Ausblick

Diese Fallstudie erzählt von einem DAX-Konzern, der durch klar priorisierte Cyber-Fitness Übungen einen großen Berg an Schwachstellen abtragen konnte. Und das ohne zusätzliche Security-Experten.

Ihr erfahrt, wie der Konzern an einer Millionen Schwachstellen aus Scannern wie Qualys, Nessus und Rapid7 nicht verzweifelte sondern durch Priorisierung Licht ins Dunkel brachte.

Ihr seht zudem den dahinterliegenden Business-Case, der mehrere EUR 100.000 pro Jahr einspart.

Über Autobahn Security

Autobahn Security ist eine SaaS-Plattform, die IT-Teams beim Priorisieren und Beheben von Schwachstellen Zeit spart und dadurch vor Hackern schützt.

Die Autobahn Plattform sammelt, filtert und priorisiert Schwachstellen aus euren Scanning-Tools und übersetzt sie in leicht verständliche Anleitungen zur Schwachstellen-Behebung – unsere Cyber-Fitness Übungen.

Autobahn Security ist das Ergebnis jahrzehntelanger Erfahrung im Bereich White-Hat-Hacking und Sicherheitsberatung für Fortune-500-Unternehmen. Autobahn Security wird branchenübergreifend von Unternehmen in über 20 Ländern eingesetzt, unter anderem von der Allianz, SwissPost und Taboola.

Ausgangslage eines Autobahn Kunden

1 Million Schwachstellen würden jedes IT-Team überfordern

Unsere Geschichte beginnt im Sicherheitsteam eines führenden DAX-Konzern. Der Konzern setzt einen bekannten Schwachstellen-Scanner ein um Sicherheitslücken in internen und externen Produktionsnetzwerken zu erkennen.

Der Scanner entdeckt eine sehr große Anzahl Schwachstellen. Dadurch fühlen sich die IT-Admins, welche die Schwachstellen beheben sollen, überfordert. Der Aufwand scheint erdrückend und weder die Security-Experten noch die Admins wissen, woher sie die Zeit und das Wissen nehmen sollten, das für eine effektive Priorisierung und Behebung einer so großen Anzahl von Schwachstellen erforderlich ist.

Die Lösung

Bündelung und Priorisierung von Sicherheitslücken in Cyber-Fitness Übungen

Anstatt 1 Million Schwachstellen einzeln zu lösen, entschied sich das Team für ein Tool, das Scan-Ergebnisse in umsetzbare Schritte gruppiert und priorisiert, um dann die eigentlichen Ursachen beheben zu können.

Autobahn Security nimmt Scanergebnisse auf, gruppiert und de-dupliziert sie und lässt sie durch unsere Priorisierungs-Engine laufen. Aus diesen Ergebnissen berechnen wir einen Hackability Score - und geben Schritt-für-Schritt-Anleitungen -- unsere Cyber-Fitness Workouts -- um den Score zu verbessern.

Das Team setzt Autobahn seit mittlerweile zwei Jahren ein und konnte bereits im ersten Monat mit einer Handvoll Behebungsmaßnahmen messbare und signifikante Fortschritt in der IT-Sicherheit aufzeigen.

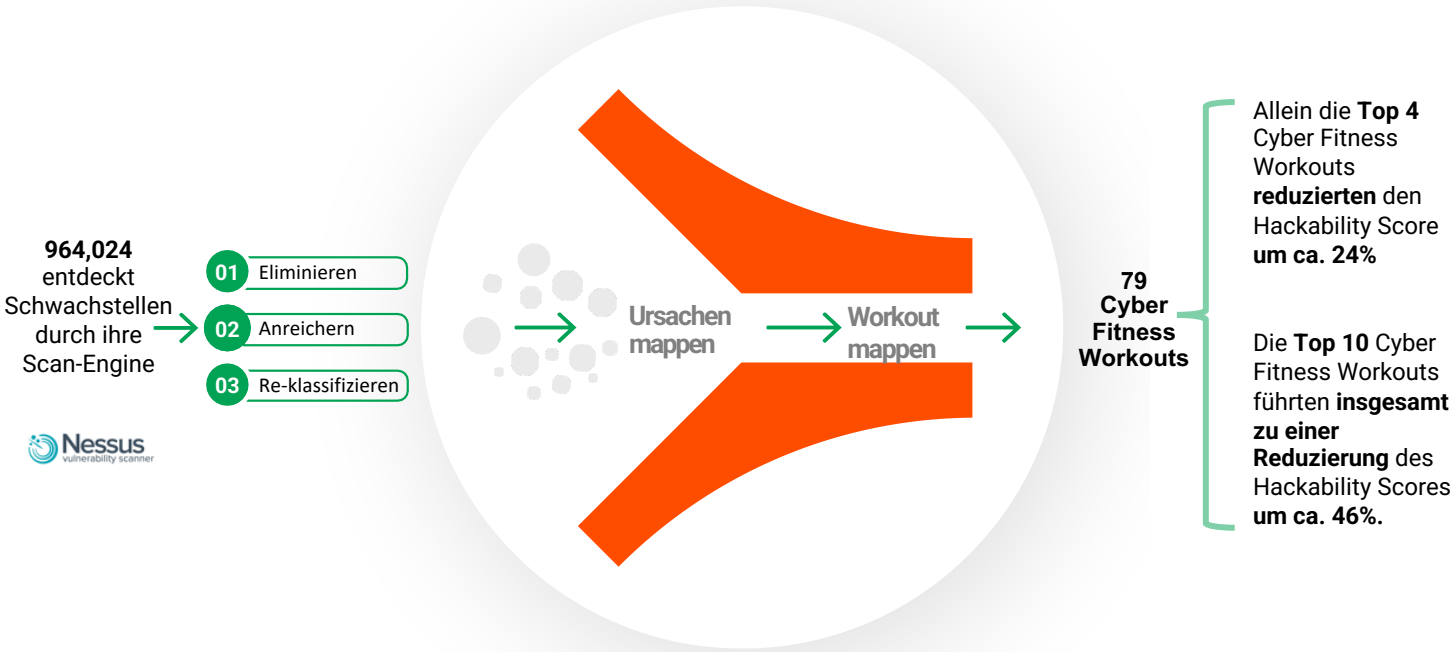
Die Top-4 Cyber-Fitness Übungen reduzierten den Hackability Score um 24%

Auf Basis der Scanergebnisse identifizierte Autobahn kritische Probleme wie vergessenes Middleware-Patching und Hardening-Lücken rund um Red-Hat-Linux. Insgesamt wurden im ersten Monat die Sicherheit von 720 IT-Systeme verbessert auf denen bis zu Dutzende Patches oder Hardening-Einstellungen fehlten. Diese Verbesserung wurde mit gerade einmal drei Cyber-Fitness Workouts erreicht, welche jeweils ein Bündel an Systemen und Problemen auf einmal angehen.

Der externe Scan zeigte ebenfalls klares Verbesserungspotential. Mit einem einzigen Workout von Autobahn - dem Patchen einer Webserver-Implementierung in einem extern erreichbaren Netzwerk – ging der Hackability-Score um 11% runter.

Die insgesamt 4 Cyber-Fitness Übungen des ersten Monats haben die Hackability um 24% gesenkt

Nach den Top 10 Cyber Fitness Übungen war der Hackability Score bereits um 46% gesunden.



Hast Du Schwierigkeiten bei der Bewertung und Priorisierung von Cybersicherheits-lücken?

Es gibt einen besseren Weg. Lass die Hunderttausenden von Sicherheitslücken, die von Qualys, Nessus, Rapid7 und anderen Schwachstellenanalyse-Tools entdeckt wurden, durch die Aggregations- und Priorisierungs-Engine von Autobahn Security laufen. Verwandele eine überwältigende Liste von To-Dos auf intelligente Weise in einige wenige Workouts, die benutzerfreundlich, einfach zu befolgen und von Experten überprüft wurden. Cyber Fitness Workouts sind so konzipiert, dass sie auch von Nicht-Sicherheitsexperten durchgeführt werden können, so dass Dein Behebungsplan besser skaliert.

Möchten Sie erfahren, wie auch IT-Fachleute, die keine Sicherheitsexperten sind, erkannte Sicherheitslücken und Fehlkonfigurationen beheben können?

Expertengespräch buchen

Wie Dein IT-Team auf einfache Weise priorisierte Lösungen anwendet

Das bloße Scannen Deiner IT-Ressourcen und das Erkennen von Sicherheitsrisiken macht Dein Unternehmen noch nicht sicher.

Eine erfolgreiche Behebung hängt von einem guten Plan zur Risikopriorisierung ab, der die Auswirkungen der Behebung auf die Sicherheitslage Deines Unternehmens berücksichtigt. Das Priorisierungssystem von Autobahn Security ordnet die Schwachstellen danach, wie leicht sie aus der Sicht eines Hackers auszunutzen sind.

Dann kommen die Cyber Fitness Workouts von Autobahn Security ins Spiel. Diese intuitiven Schritt-für-Schritt-Anleitungen zeigen Dir, wie Du die wichtigsten Schwachstellen beheben kannst - und sind so geschrieben, dass Du sie an die IT-Verantwortlichen schicken kannst, damit diese sie selbst umsetzen.

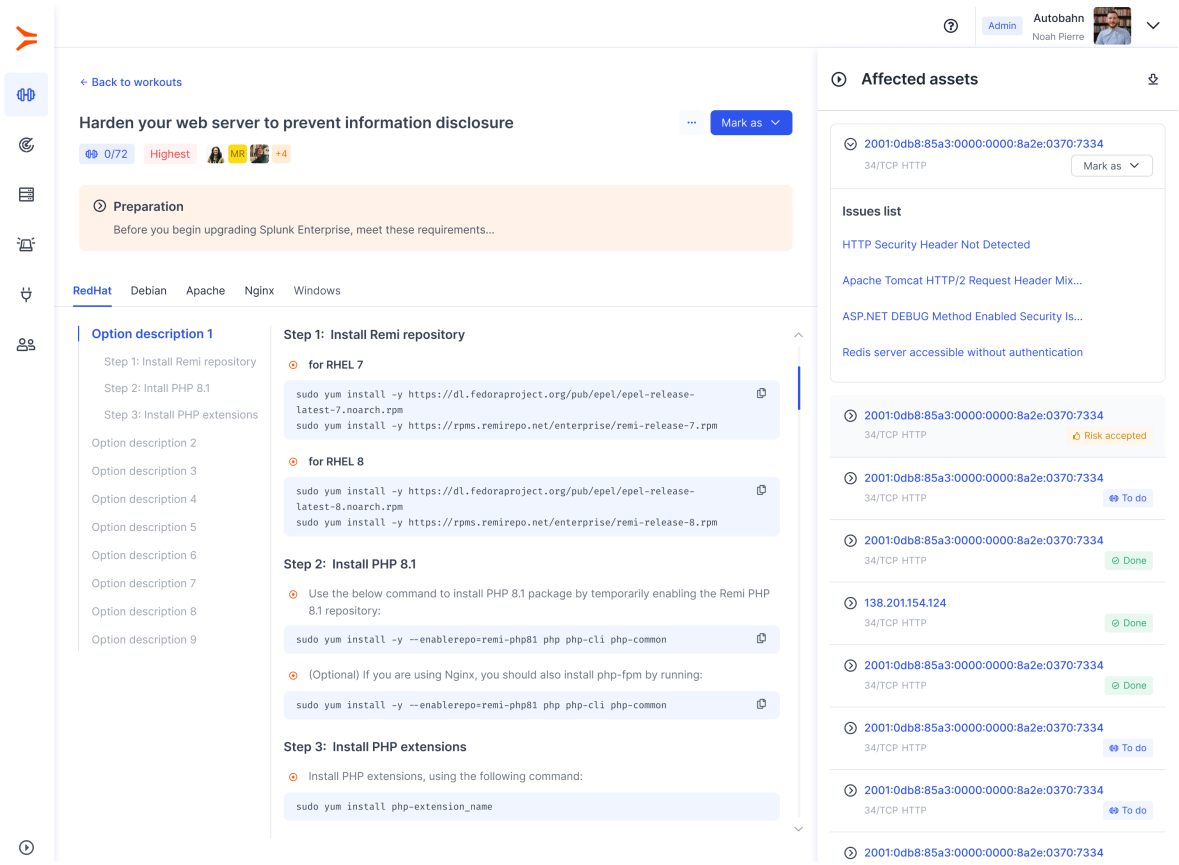


Abbildung 2.

Ein Beispiel für ein Cyber Fitness Workout in der Autobahn Security Plattform. Jedes Workout gibt einen Überblick über den Aufwand, den es erfordert - und wie sehr sich jedes Workout auf die Hackability Ihrer Organisation auswirken wird.

Obwohl das Spektrum möglicher Angriffe breit gefächert ist, kannst Du oft mehrere Schwachstellen durch die Installation eines einzigen Patches oder die Änderung einiger weniger Einstellungen beheben. Die von Autobahn Security entwickelten Cyber-Fitness-Workouts erklären, wie Du genau das tun kannst: welche spezifischen Schritte entscheidend sind, um Dein Unternehmen sicherer zu machen.

Zur Veranschaulichung: Ein Patching-Workout enthält oft einen Schritt, der Dir zeigt, wo Du die neueste stabile Softwareversion erhälst. Außerdem kann das Workout Dir sagen, welche Systemvoraussetzungen bei der Aktualisierung zu beachten sind - oder wie Du ein Backup erstellst. Workouts geben auch Tipps zur Automatisierung von Aktualisierungen - oder zur Rücknahme von Aktualisierungen - und geben die richtige Reihenfolge für die Aktualisierung bestimmter Komponenten an.

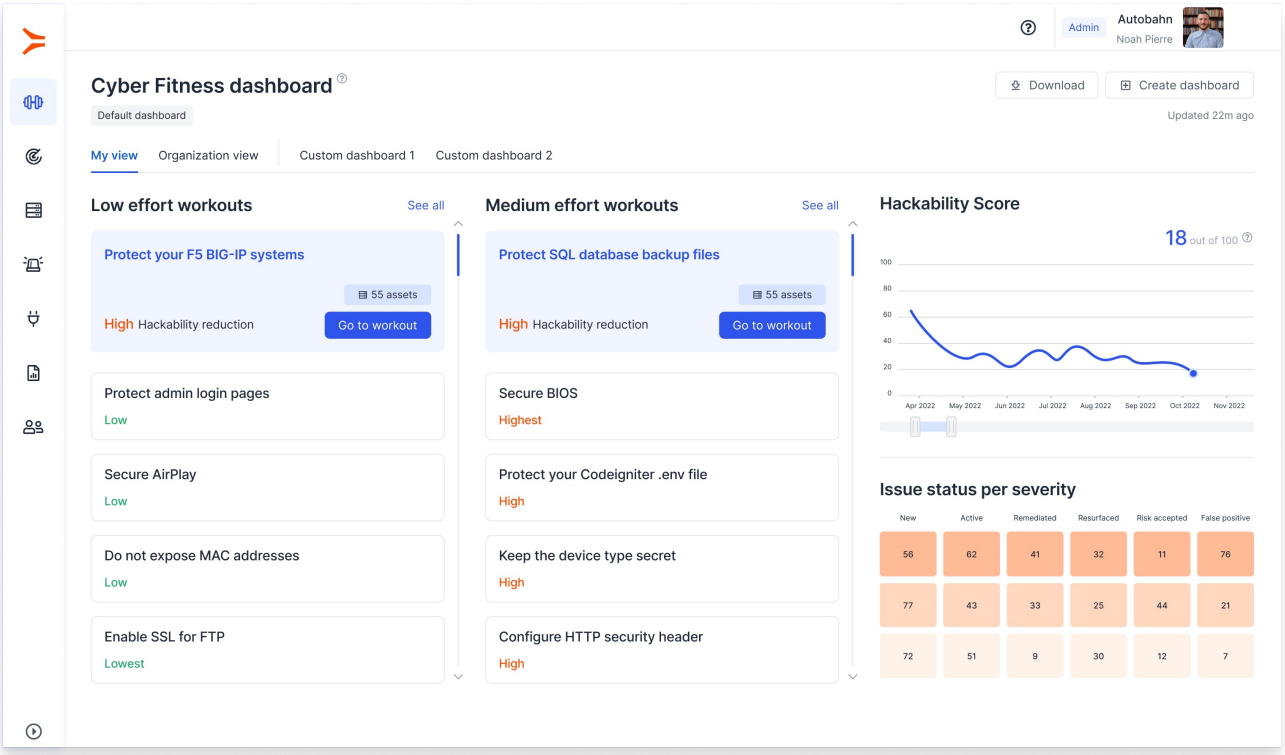


Abbildung 3.

Ein Beispiel für die Schritte, die in einem Cyber Fitness Workout auf der Autobahn-Plattform enthalten sind. Jede Anleitung ist so geschrieben, dass es auch für Nicht-Sicherheitsexperten verständlich (und umsetzbar) ist.

Die Plattform ist darauf ausgelegt, Deinem IT-Team die Arbeit so einfach wie möglich zu machen: Ausgestattet mit den notwendigen Korrekturen muss es nur noch die bereitgestellten Lösungen anwenden.

Außerdem kannst Du ganz einfach Aufgaben an ein Ticketing-System senden, um den Fortschritt der Behebung zu verfolgen. Jedes Cyber Fitness Workout reduziert Deinen Hackability Score und verbessert die Sicherheitslage kontinuierlich.

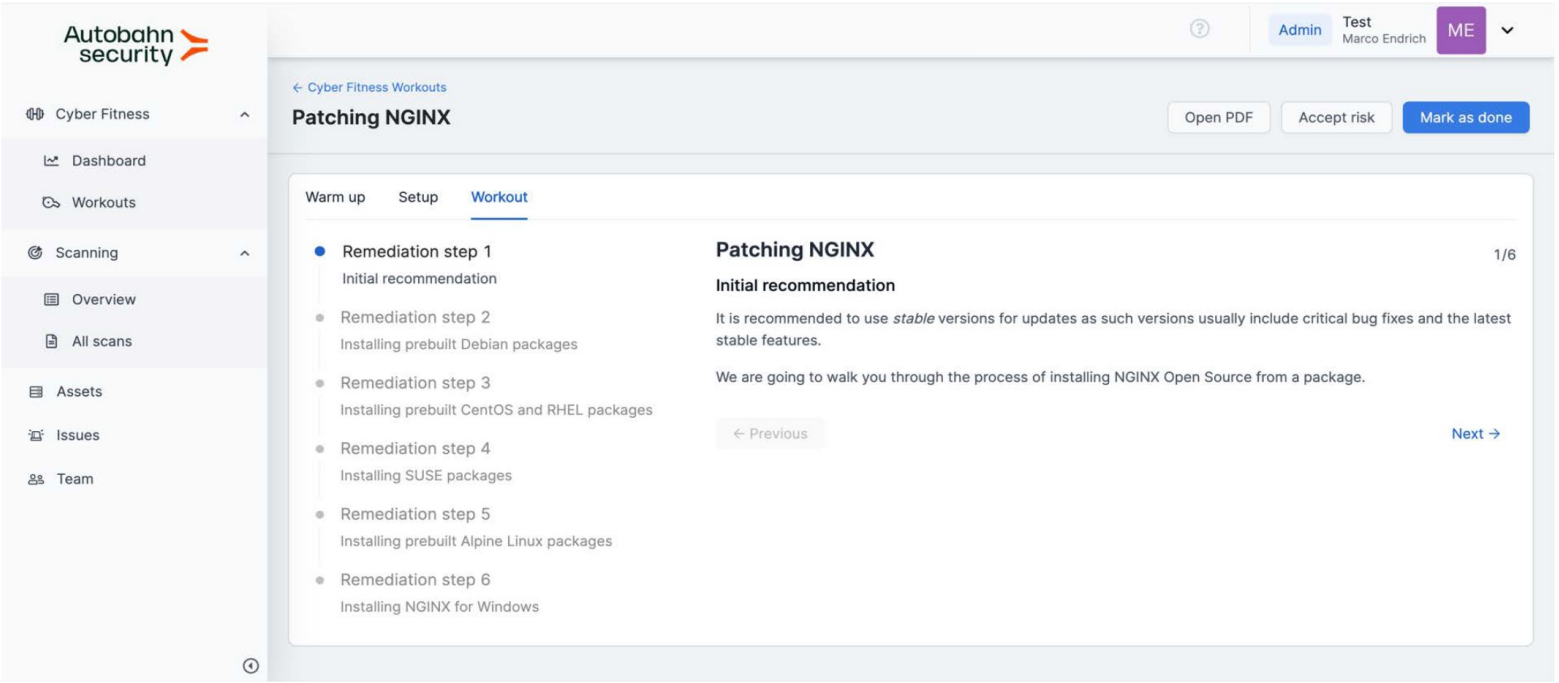


Abbildung 4.

Ein weiteres Beispiel für die Schritte, die in einem Cyber-Fitness-Workout auf der Autobahn-Plattform enthalten sind. Jedes Workout ist detailliert und so geschrieben, dass es auch für Nicht-Sicherheitsexperten verständlich (und umsetzbar) ist.

Schwachstellen leicht behoben: 5+1 Dinge, die Sie über Cyber Fitness Workouts wissen sollten

Jetzt weiterlesen

Business Case: EUR 270.000 jährliche Einsparung für einen großen Mittelständler

Effektive Sicherheitsmaßnahmen können zwei finanzielle Ziele erreichen:

1. Verringerter manueller Aufwand

Durch klare Priorisierung und einfach verständliche Cyber Fitness Übungen entfallen manuelle (und oft monotone) Prozessschritte, vorhandene Kapazitäten werden sinnvoller eingesetzt. Hierauf konzentriert sich die Return-of-Investment-Berechnung der nächsten Seiten

2. Geringe Kosten durch Hacking-Vorfälle

Die Anzahl und Kosten von Hacking-Vorfällen variieren stark zwischen Firmen. Daher versuchen wir eine Abschätzung mit Durchschnittswerten gar nicht erst.

Diese Datenpunkte sollten euch aber bei der individuellen Abschätzung helfen können:

- Nach Angaben von Forrester kommt es bei einem durchschnittlichen Unternehmen mit einem Umsatz von USD 2 Milliarden zu 2,5 Datenschutzverletzungen pro Jahr
- Eine erhebliche Datenschutzverletzung kostet laut Forrester EUR 610 Tausend
- IBM errechnet die durchschnittlichen Gesamtkosten des zusätzlichen Reputationsverlusts mit EUR 1,4 Millionen

Berechnungs-methode

Die ROI-Berechnung basiert auf einem grossen Mittelständler.

Die Grundlage unserer Berechnungen ist der Durchschnitt von 10 unserer Kunden aus den Branchen Fertigung, Technologie, Versorgung und Finanzen erstellt.

Der Durchschnitt ergibt eine Organisation mit:

- IT-Systeme (IPs): 1.170
- Mitarbeiter: 7.500
- Davon Security-Team: 17,5
- Umsatz: EUR 3 Milliarden

Effizienz-gewinn bei Sicherheit und IT-Betrieb

Durch die Verringerung des manuellen Aufwands bei der Priorisierung von Schwachstellen und der Erstellung von Richtlinien zur Behebung von Schwachstellen erzielt Autobahn Security erhebliche Budgeteinsparungen.

	Metrik	Quelle	Betrag	Einheit
Deine Firma	Jahresgehalt IT-Security Experte	Glassdoor	71.979	EUR / Jahr
	Jahresgehalt IT-Admin/DevOps	Glassdoor	60.500	EUR / Jahr
	Anzahl der Assets	Autobahn Kundendurchschnitt	1.170	IPs
	Verfügbare Zeit für Tech-Aufgaben	60% Tech-Aufgaben	1.008	Std/Jahr
Manueller Aufwand für die Priorisierung und Behebung von Schwachstellen	Durchschnittliche Anzahl neuer Schwachstellen/IP/Monat	Autobahn Kundendurchschnitt (Netzwerk + authentifizierte Schwachstellen-Scans)	0,79	Vulns
	Zeit für Priorisierung einer Schwachstelle	Kundenschätzung	27	min
	Anzahl der kritischen Ergebnisse	Kundendurchschnitt	3%	
	Zeit, um Lösungen für eine Schwachstelle zu recherchieren	Kundenschätzung	68	min
	Zeit, um Schwachstellen durch Sicherheitsexperten zu priorisieren	(von oben abgeleitet)	4.991	Std/Jahr
	Zeit, um Lösungen durch IT-Admins/DevOps zu recherchieren	(von oben abgeleitet)	346	Std/Jahr
	Gesamtzeit für Priorisierung und Recherche	(von oben abgeleitet)	5.337	Std/Jahr
Ersparnisse durch automatisierte Priorisierung & Unterstützung bei der Behebung	Zeitersparnis durch Priorisierung durch Autobahn	Kundenschätzung	70%	
	Zeitersparnis durch Wegfall der Recherche	Kundenerfahrung	90%	
	Zeitersparnis gesamt durch Autobahn	(von oben abgeleitet)	3.805	Std/Jahr
	Gesamtersparnis		268.162	EUR / Jahr

Dein Business Case	**Deine Vorteile**	Jahr 1	Jahr 2	Jahr 3	Total
	1- Effizienzgewinne im Betrieb	€ 268.162	€ 268.162	€ 268.162	€ 804.487
	2- Verringerung des Risikos von Datenpannen	*Individuelle Betrachtung auf Basis des Unternehmensrisiko*			
	3- Verringerung des Risikos von Imageschäden	*Individuelle Betrachtung auf Basis des Unternehmensrisiko*			
	Total	**€ 268.162**	**€ 268.162**	**€ 268.162**	**€ 804.487**

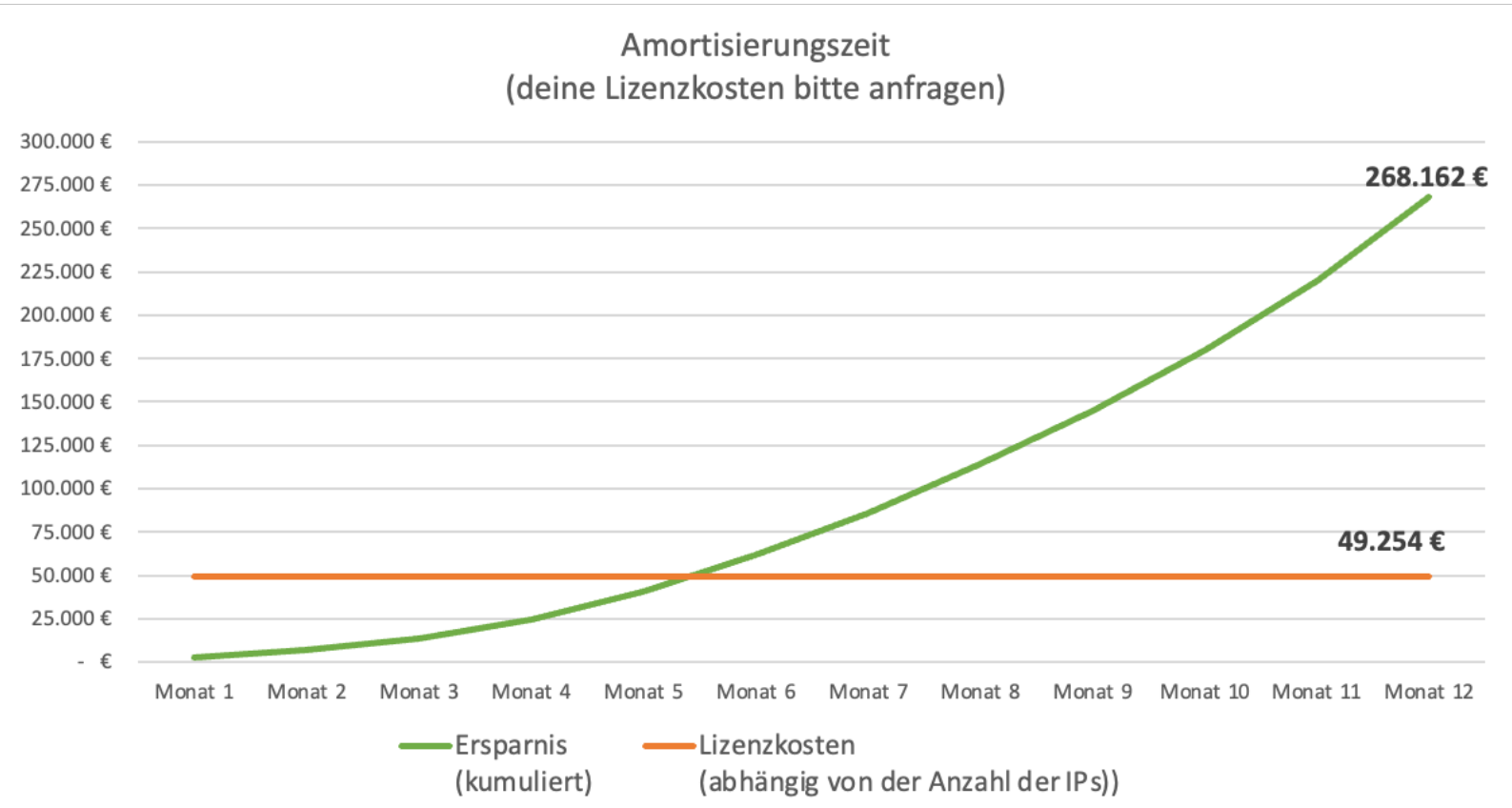
Excel zur eigenen Berechnung

Automatisierte Priorisierung macht sich innerhalb von 5,5 Monaten bezahlt

Für den Leiter eures Sicherheitsteams sind Ressourcen das wichtigste Thema.

Sicherheitsexperten zu finden ist nicht einfach; sie mit interessanter Arbeit zu versorgen genauso wenig. Durch das automatische Priorisieren von Schwachstellen fallen monotone manuelle Schritte weg, so dass sich die Hacking-Experten auf interessantere Themen wie Pentesting, Red-Teaming und Blue-Teaming konzentrieren können.

Die Zeitersparnis alleine holen die jährlichen Lizenzkosten für die Automatisierung in den ersten 5,5 Monaten heraus. Hinzu kommen eure individuellen Ersparnisse durch weniger Sicherheitsvorfälle.



Die Schlüsselzahlen

- *€270.000 – Jährliche Einsparung durch Automatisierung*
- *Zusätzlich: Individuelle Risikoreduktion*
- *3.805 – Eingesparte Stunden für eure Sicherheitsexperten*
- *30% – durchschnittliche Reduzierung der Hackability nach 90 Tagen*

Wie ihr loslegen können - und was euch innerhalb der ersten Woche erwartet

01. Lerne die wichtigsten Aspekte der SaaS-Plattform kennen

02. Wir starten gemeinsam den ersten Schwachstellen-Scan starte

03. Ihr bekommt das erste Paket and priorisierten Cyber-Fitness Übungen

04. Gemeinsam mit unserem Cyber-Fitness Coach besprecht ihr die Ergebnisse und arbeitet an den Cyber-Fitness Übungen

Wir stehen für eine erste Konsultation gerne zur Verfügung

Im ersten Gespräch wird einer unsere Cyber-Fitness Coaches eure individuellen Herausforderungen besprechen, euch einen kurzen Produktüberblick geben und mögliche nächste Schritte besprechen.

Ihr bekommt natürlich auch kostenlosen und unverbindlichen Test-Zugang zur Plattform.

Wir helfen gerne im persönlichen Gespräch, eure individuelle Risikoreduktion zu quantifizieren