



EXPERT
PAPER

How a DAX company dealt with 1 million vulnerabilities

Includes assistance for your ROI calculation

Outlook

This case study describes the experience of a DAX company that was able to eliminate a large mountain of vulnerabilities through clearly prioritized Cyber Ffitness Workouts, without the need for additional security experts.

Learn how the company did not despair of a million vulnerabilities from scanners such as Qualys, Nessus and Rapid7, but instead shed light on them through prioritization.

You will also learn about the underlying business case, which saves several EUR 100,000 per year.

01. [1 million vulnerabilities. What now?](#)
02. [Reduce Hackability Score by 24% with just 4 Cyber Fitness Workouts](#)
03. [The business case with clear ROI](#)



About Autobahn Security

Autobahn Security is a SaaS platform that saves IT security professionals time – and empowers IT teams to make their networks more secure.

Our platform aggregates, filters and prioritizes vulnerabilities from multiple scanners and turns them into easy-to-understand remediation guides.

Autobahn Security is the result of decades of white-hat hacking and security consulting experience for Fortune 500 companies. Autobahn Security is trusted by companies across multiple industries in over 20 countries, including Allianz, SwissPost and Taboola.

The situation of the Autobahn customer in the beginning

1 million vulnerabilities would
overwhelm any IT team

Our story begins in the security team of a leading DAX corporation. The corporation relies on a **well-known vulnerability scanner** to detect security issues in internal and external production networks.

The scanner detects 1 million vulnerabilities. As a result, the IT admins who are supposed to fix the vulnerabilities feel overwhelmed. The effort seems not feasible and neither the security teams nor the admins know **where to find the time and knowledge needed to effectively prioritize and remediate** such a large number of vulnerabilities.



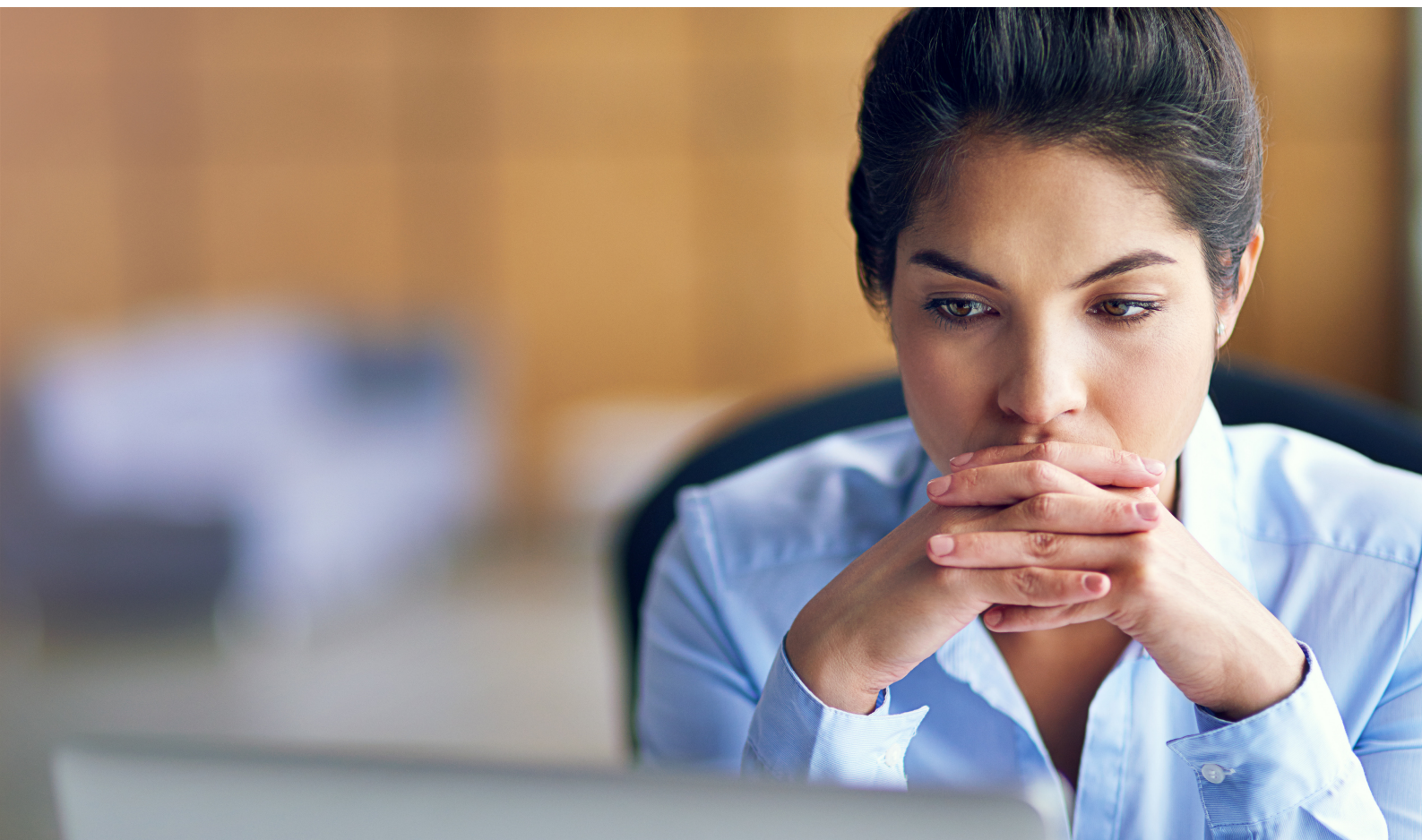
The solution

Consolidating and prioritizing security vulnerabilities in Cyber Fitness Workouts

Instead of solving 1 million vulnerabilities one by one, the team opted for a platform that **groups and prioritizes scan results into easy-to-implement steps** to address the root causes - rather than analyzing each vulnerability individually.

Autobahn Security takes scan results, groups and de-duplicates them, and runs them through **our prioritization engine**. From these results, we calculate the **Hackability Score** and provide step-by-step instructions - our **Cyber Fitness Workouts** - to improve the score within the Cyber Fitness Journey.

The team has been using Autobahn Security for two years now and was able to demonstrate **measurable** and **significant progress** in IT security with a handful of remediation actions in the first month.



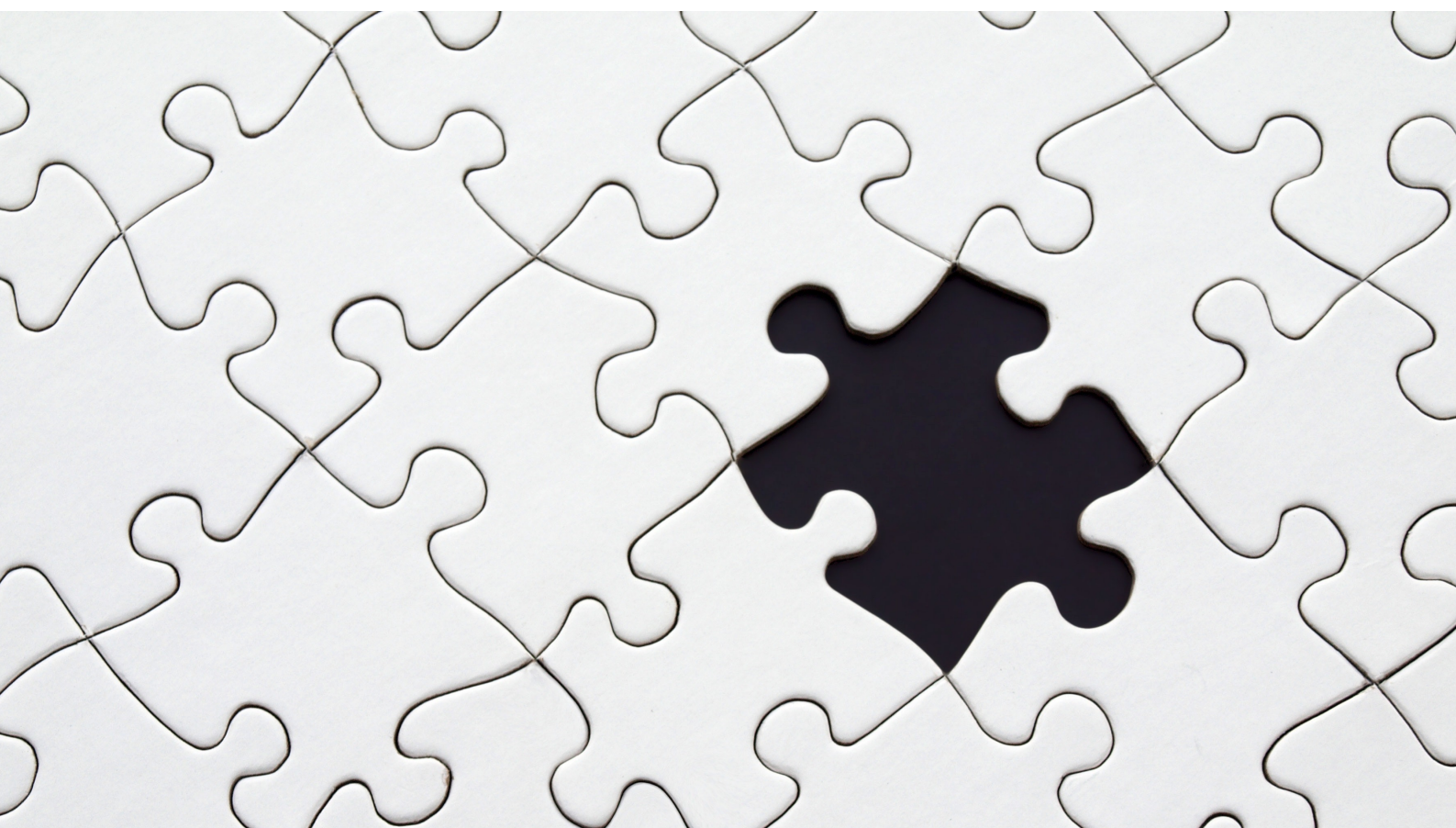
The top 4 Cyber Fitness Workouts reduced the Hackability Score by 24%

Based on the scan results, Autobahn identified critical issues such as forgotten middleware patching and hardening gaps around Red Hat Linux. In total, the resilience of **720 IT systems**, each missing up to dozens of patches or hardening settings, was improved in the first month. This improvement was achieved with just three Cyber Fitness Workouts, each addressing a bundle of systems and issues at once.

The external scan also showed clear potential for improvement. With a single Workout from Autobahn - patching a web server implementation in an externally accessible network - the Hackability Score went down by 11%.

The total of 4 Cyber Fitness Workouts in the first month lowered Hackability by 24%

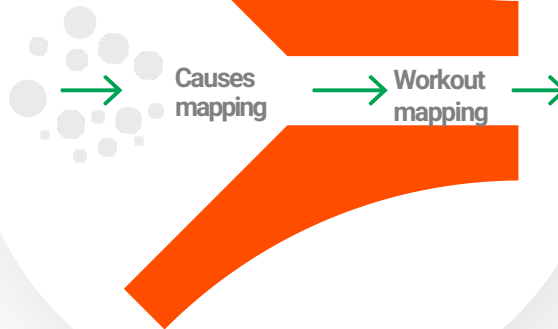
After the **top 10 Cyber Fitness Workouts**, the **Hackability Score was already enhanced by 46%**



964,024
vulnerabilities
discovered
through scan
engine



- 01 Eliminate
- 02 Enrich
- 03 Re-classify



79
Cyber
Fitness
Workouts

The **Top 4** Cyber Fitness Workouts alone **reduced** the Hackability Score **By approx. 24%**

The **Top 10** Cyber Fitness Workouts **overall reduced** Hackability Score **by approximately 46%**.

Having trouble assessing and prioritizing cybersecurity gaps?

There's a better way. Run the hundreds of thousands of vulnerabilities discovered by Qualys, Nessus, Rapid7 and other vulnerability assessment tools through **Autobahn Security's aggregation and prioritization engine**. Intelligently transform an overwhelming list of to-dos into **a few Workouts** that are user-friendly, easy to follow, and peer-reviewed. Cyber Fitness Workouts are designed to be **executed by non-security experts**, so your remediation plan scales better.

Want to learn how IT professionals can fix security vulnerabilities and misconfigurations more efficiently?

[Book a Consultation](#)

How your IT team easily applies prioritized solutions

Simply scanning your IT assets and identifying security risks does not make your organization secure.

Successful remediation depends on a **good risk prioritization plan** that considers the impact of remediation on your organization's security posture. Autobahn Security's **prioritization system** ranks vulnerabilities based on how easy they are to exploit from a **hacker's perspective**.

That's when Autobahn Security's Cyber Fitness Workouts come into play. These **intuitive step-by-step guides** show you how to fix the most important vulnerabilities - and are written so you can send them to IT leaders to implement on their own.

Harden your web server to prevent information disclosure

... [Mark as](#)

0/72 Highest +4

🕒 Preparation

Before you begin upgrading Splunk Enterprise, meet these requirements...

[RedHat](#) [Debian](#) [Apache](#) [Nginx](#) [Windows](#)

Option description 1

Step 1: Install Remi repository

Step 2: Install PHP 8.1

Step 3: Install PHP extensions

Option description 2

Option description 3

Option description 4

Option description 5

Option description 6

Option description 7

Option description 8

Option description 9

Step 1: Install Remi repository

⦿ for RHEL 7

```
sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
sudo yum install -y https://rpms.remirepo.net/enterprise/remi-release-7.rpm
```

⦿ for RHEL 8

```
sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
sudo yum install -y https://rpms.remirepo.net/enterprise/remi-release-8.rpm
```

Step 2: Install PHP 8.1

- ⦿ Use the below command to install PHP 8.1 package by temporarily enabling the Remi PHP 8.1 repository:

```
sudo yum install -y --enablerepo=remi-php81 php php-cli php-common
```

- ⦿ (Optional) If you are using Nginx, you should also install php-fpm by running:

```
sudo yum install -y --enablerepo=remi-php81 php php-cli php-common
```

Figure 1.

An example of a Cyber Fitness Workout in the Autobahn Security platform. Each Workout provides an overview of the effort it requires - and how much each Workout will impact your organization's Hackability.

Although the spectrum of possible attacks is broad, you can often fix multiple vulnerabilities by installing a single patch or changing a few settings. The **Cyber Fitness Workouts** developed by Autobahn Security **explain how you can do just that**: what specific steps are critical to making your organization more secure.

To illustrate, a patching Workout often includes a step that shows you where to get **the latest stable software version**. In addition, the workout may tell you what **system requirements** to consider when updating - or how to create a **backup**. Workouts also give tips on **how to automate updates** - or roll back updates - and give the correct order for updating certain components.

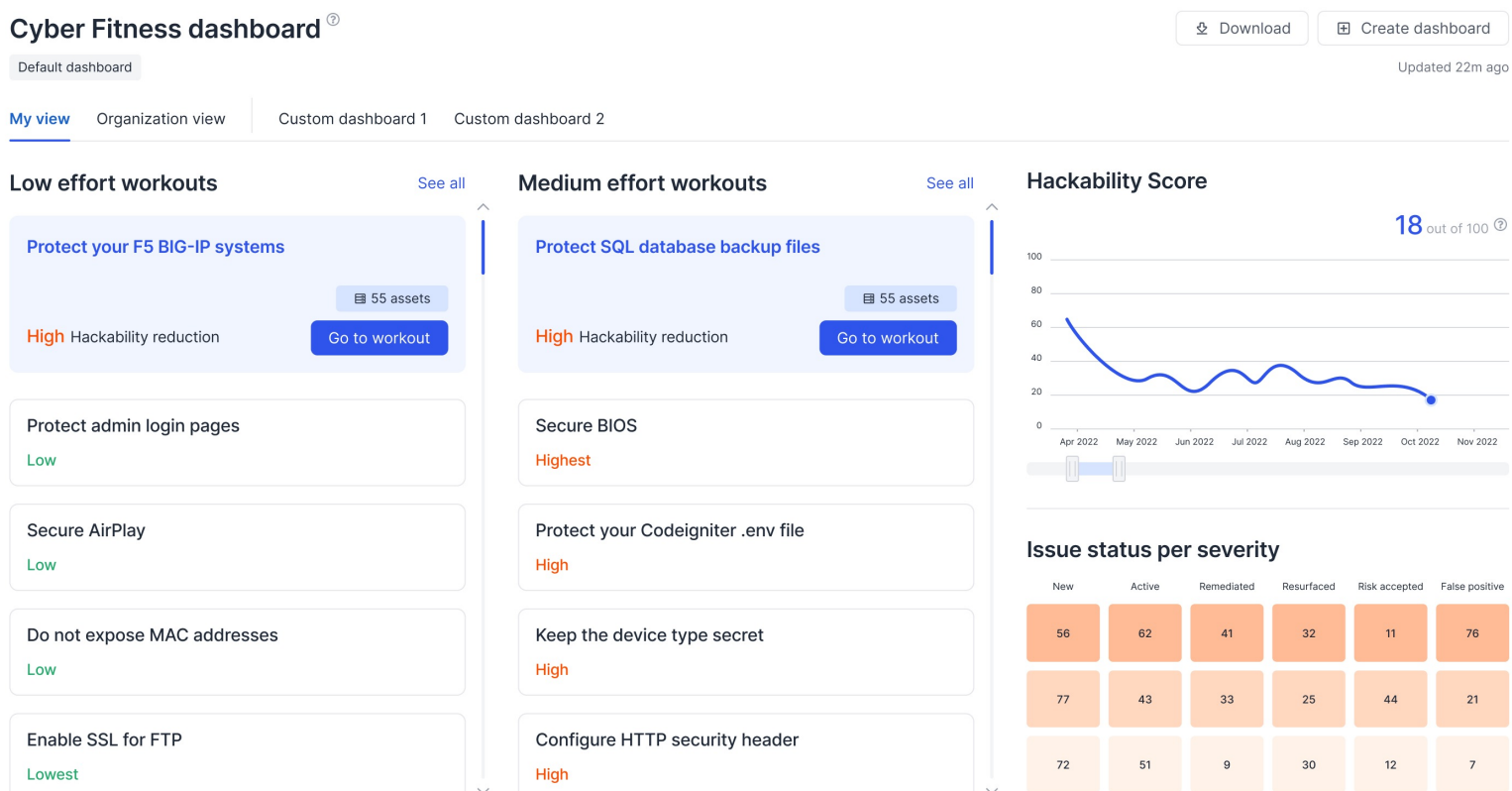


Figure 2.

An example of the steps included in a Cyber Fitness Workout on the Autobahn platform. Each tutorial is written in a way that is understandable (and actionable) for non-security experts

The platform is designed to **make your IT team's job as easy as possible**: Equipped with the necessary fixes, all they have to do is apply the solutions provided.

Plus, you can easily send tasks to a **ticketing system** to track remediation progress. Each Cyber Fitness Workout reduces your **Hackability Score** and continuously improves the security posture.

← Cyber Fitness Workouts

Secure SSH

Download workout

Send to Jira

Mark workout as ▾

Warm up Setup **Workout**

• Remediation step 1

Batch download assistant

• Remediation step 2

Set up OPatch utility

• Remediation step 3

Description

• Remediation step 4

Description

• Remediation option N: Insert title here

Description

• Remediation option N: Insert title here

Description

Mitigation step 1 - Authentication

After creating the SSH key pair, you can safely disable password authentication. However, make sure your key-based authentication is set up properly. Verify that you can log in using the authentication key.

☒ 1.1 - Log in to the server using SSH keys

```
ssh remote_username@server_ip_address
```

☐ 1.2 - Open the SSH configuration either as a root user or as a user with sudo privileges Run the following command in the Terminal:

```
sudo vim /etc/ssh/sshd_config
```

☐ 1.3 - Find the "PasswordAuthentication" line and set it to "no"

Edit the file with your preferred text editor and set the PasswordAuthentication to no as shown below:
PasswordAuthentication no

ⓘ Note

Do not forget to uncomment the line if the # is present

☐ 1.4 - Restart the SSH service to apply the new configuration

```
sudo systemctl restart sshd
```

Figure 3.

Another example of the steps included in a Cyber Fitness Workout on the Autobahn platform. Each Workout is detailed and written in a way that is understandable (and actionable) even for non-security experts..

5+1 things to know about cyber fitness workouts

[Read more now](#)

Business Case: **EUR 270.000** annual **savings** for large to medium-sized companies

Effective security measures can achieve two financial goals.:

1. Reduced manual effort

Clear prioritization and easy-to-understand Cyber Fitness Workouts eliminate manual (and often monotonous) process steps. Existing capacity is used more wisely. This is the focus of the Return of Investment calculation on the following pages.

2. Lower cost resulting from hacking incidents

The number and costs of hacking incidents vary greatly between companies. Therefore, we do not even attempt an estimate with average values.

However, these data points should help you with your individual estimation.:

- According to Forrester, the average company with \$2 billion in revenue experiences **2.5 data breaches per year**
- According to Forrester, a significant **data breach** costs **EUR 610,000**
- IBM calculates the average total cost of the additional **loss of reputation at EUR 1.4 million**

Calculation method

The ROI calculation is based on a large to mid-sized companies.

The basis of our calculations is the average created by 10 of our customers from the manufacturing, technology, utilities and finance industries.

The average results in an organization with:

- IT-Systems (IPs): 1.170
- Employees: 7.500
- of which is Security Team: 17,5
- Turn over: 3 Billion EUR

Efficiency gains in Security and IT operations

By reducing the manual effort required to prioritize vulnerabilities and create remediation policies, Autobahn Security achieves significant budget savings.

	Metrics	Source	Amount	Unit
Your company	Annual salary IT Security Expert	Glassdoor	71.979 EUR / Year	
	Annual salary IT Admin/DevOps	Glassdoor	60.500 EUR / Year	
	Number of Assets	Autobahn customer avergae	1.170 IPs	
	Available time for tech tasks	60% Tech tasks	1.008 Hrs / Year	
Manual effort for prioritization and remediation of vulnerabilities	Average number of new vulnerabilities/IP/month	Autobahn customer avergae (Network + authenticated vulnerability scans)	0,79 Vulns	
	Time for prioritization of a vulnerability	Customer estimate	27 min	
	Number of critical results	Customer average	3%	
	Time to research solutions for a vulnerability	Customer estimate	68 min	
	Time to prioritize vulnerabilities by security experts	(Derived from above)	4.991 Hrs / Year	
	Time to research solutions through IT admins/DevOps.	(Derived from above)	346 Hrs / Year	
	Total time for prioritization and research	(Derived from above)	5.337 Hrs / Year	
Savings through automated prioritization & remediation support	Time saving through prioritization by Autobahn	Customer estimate	70%	
	Time saving due to elimination of research	Customer experience	90%	
	Total time savings due to Autobahn	(Derived from above)	3.805 Hrs / Year	
Total savings			268.162 EUR / Year	

Excel to make your own calculation

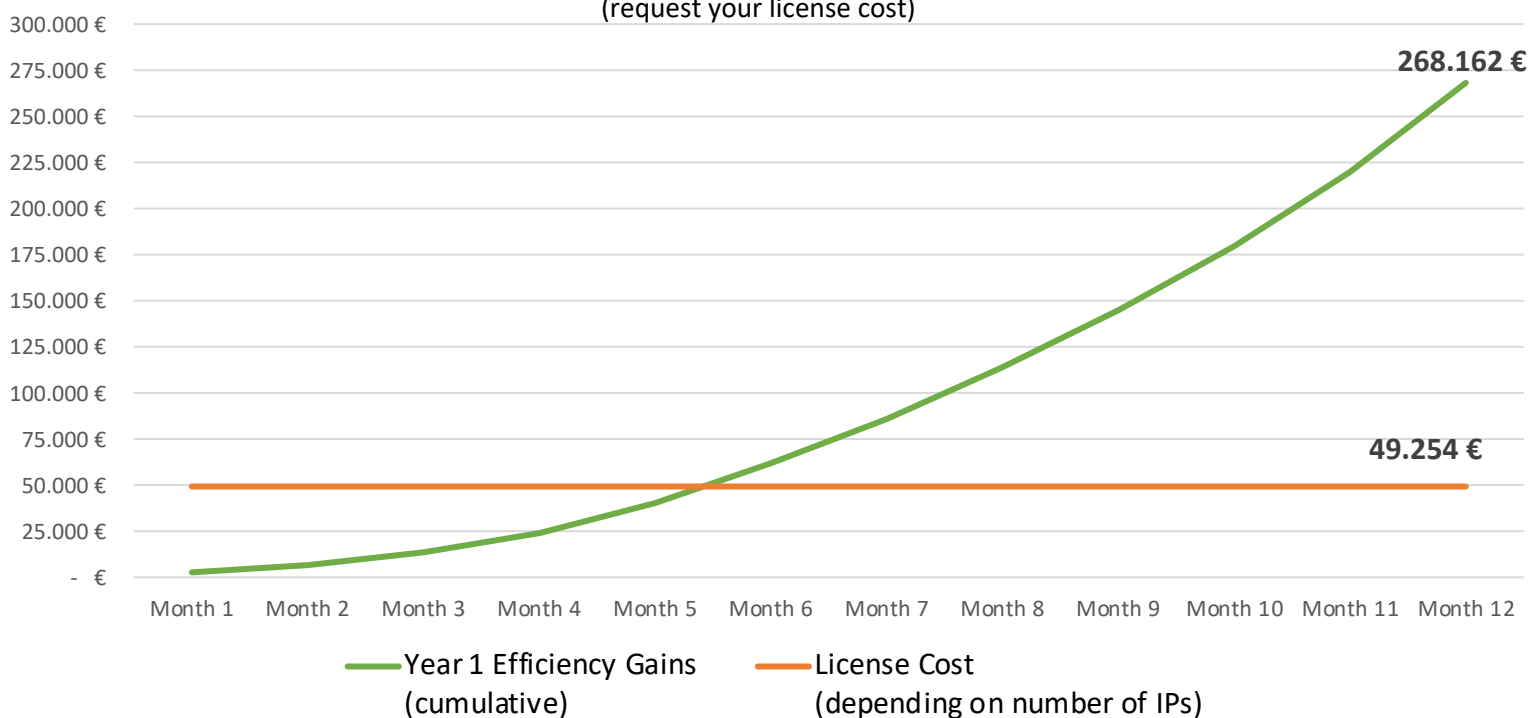
Automated prioritization pays off within 5.5 months

Finding security experts isn't easy; neither is providing them with interesting work. Automatic vulnerability prioritization eliminates monotonous manual steps, allowing hacking experts to focus on more interesting topics like pentesting, red-teaming, and blue-teaming.

The time savings alone will pay off the annual licensing cost for automation with the first 5.5 months. Add to that your individual savings from fewer security incidents.

	Benefit	Year 1	Year 2	Year 3	Total
		€ 268.162	€ 268.162	€ 268.162	€ 804.487
Your business case	1- Security operations efficiency gains				
	2- Reduction in risk of data breaches	As per individual company risk			
	3- Reduction in reputational damage	As per individual company risk			
Total		€ 268.162	€ 268.162	€ 268.162	€ 804.487

Time to value
(request your license cost)



The key figures

- 3,805 - Hours saved for your security experts
- > €200,000 - **Annual savings** through automation
- 30% - average Hackability reduction after 90 days
- Thereby individual risk reduction due to **fewer incidents**

How you get started - and what to expect from us within the first week

01. Learn the most important aspects of the SaaS platform
02. We start the first vulnerability scan together
03. You will get the first package of prioritized Cyber Fitness Workouts
04. Together with our Cyber Fitness Coach you will discuss the results and work on the Cyber Fitness Workouts

We are available for a personal consultation

During the initial consultation, one of our Cyber Fitness Coaches will discuss your individual challenges, give you a brief product overview, and discuss possible next steps.

You will of course also get free and non-binding test access to the platform.



We will be happy to help you quantify your individual risk reduction in a personal meeting.