Autobahn security

Case Study

Vulnerability Management Made Easy.

How you can handle 1 million security issues with just 80 actionable workouts

Too many cybersecurity issues generally overwhelm IT staff in remediating the root causes of these flaws. Read in this case study in just 5 minutes how one client could handle 1 million issues detected by vulnerability scanners like Qualys, Nessus or Rapid7 with just 80 actionable workouts that are user-friendly, easy to follow, and expert approved. Sounds interesting? In a free expert meeting, we evaluate your individual challenges and provide an overview of our process and potential next steps.

About Autobahn Security

Autobahn Security takes the thousands of vulnerabilities your cyber scanner reveals and turns them into actionable steps. With automated prioritization, you save up to 90% of time spent on remediation management. Autobahn is currently trusted by companies across different industries in over 20 countries, including Allianz & SwissPost.

The problem: Why 1 million detected cybersecurity issues predictably overwhelm any IT team

The story began as a typical vulnerability assessment journey many IT professionals are familiar with. In our case study, the customer – a leading software manufacturer – uses a well-known vulnerability scanner to detect security issues in their internal and external production networks.

As the scanner discovered close to 1 million issues, the customer's IT team felt predictably overwhelmed. They knew all too well how much effort and expert knowledge would be required to perform effective remediation.

The solution: Cluster & prioritize these issues into actionable steps fixing root causes

The most practical solution to make issue remediation manageable would be to cluster and prioritize these 1 million issues into actionable steps that fix root causes. That's why the team began searching for software tools and SaaS platforms that could provide such a solution.

At this stage, Autobahn Security got involved and identified workouts that were likely to greatly affect the customer's production networks. It turned out that just two workouts in two production networks would solve over 40% of the company's total hackability problems.

Just 3 critical issues contributed to 50% of the company's total hackability

From the internal scan, Autobahn Security was able to identify 720 production environments with critical or high severity issues. And in perfect sync with the other related findings, only three of these critical issues contributed to 50% of the company's total hackability – those were mostly Red Hat Linux patching issues in the internal network.

The external scan also brought energizing results. By doing one of Autobahn's workouts for patching a web-server implementation in one externally reachable network, the customer could solve over 15% of external vulnerabilities.
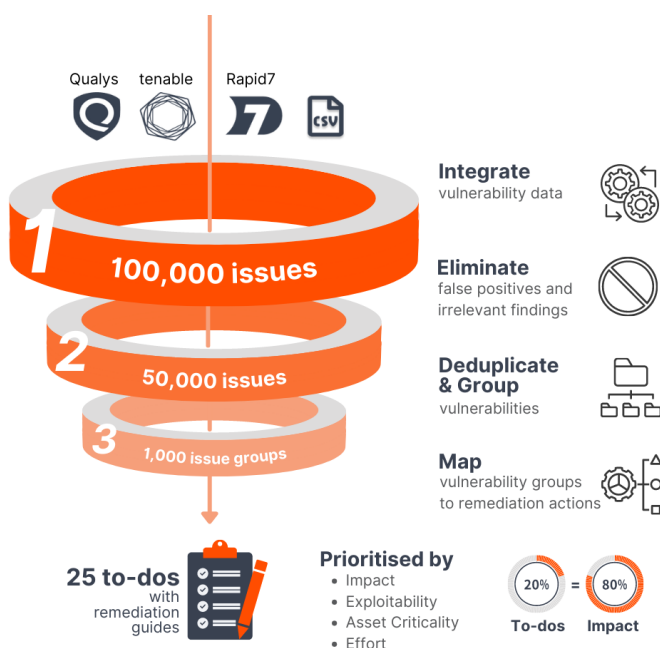

Figure 1. With Autobahn, 100,000 issues become 25 Workouts. Autobahn imports data from different sources and processes it by eliminating false positives, deduplicating and grouping the issues, and assigning them to Cyber Fitness Workouts.

Do you face difficulties in evaluating and prioritizing cybersecurity issues in your company?

Just let the hundreds of thousands of issues detected by Qualys, Nessus, Rapid7 and other reputable vulnerability scanners pass through Autobahn's aggregation and prioritization funnel to distill the ocean of trouble into a few workouts that are user-friendly, easy to follow, and expert approved.

> You want to find out how even non-security IT professionals can remediate those detected security flaws and misconfigurations?
>
> **Book a free expert call ⟶**

How your IT team can easily apply prioritized solutions

To be able to scan your IT assets and identify security risks does not make your company secure just yet. Successful remediation relies on a good risk prioritization plan that would consider the impact of remediation on your organization's security posture. Companies must order the identified risks by level of criticality. This is where Autobahn Security's Cyber Fitness Workouts come into play.
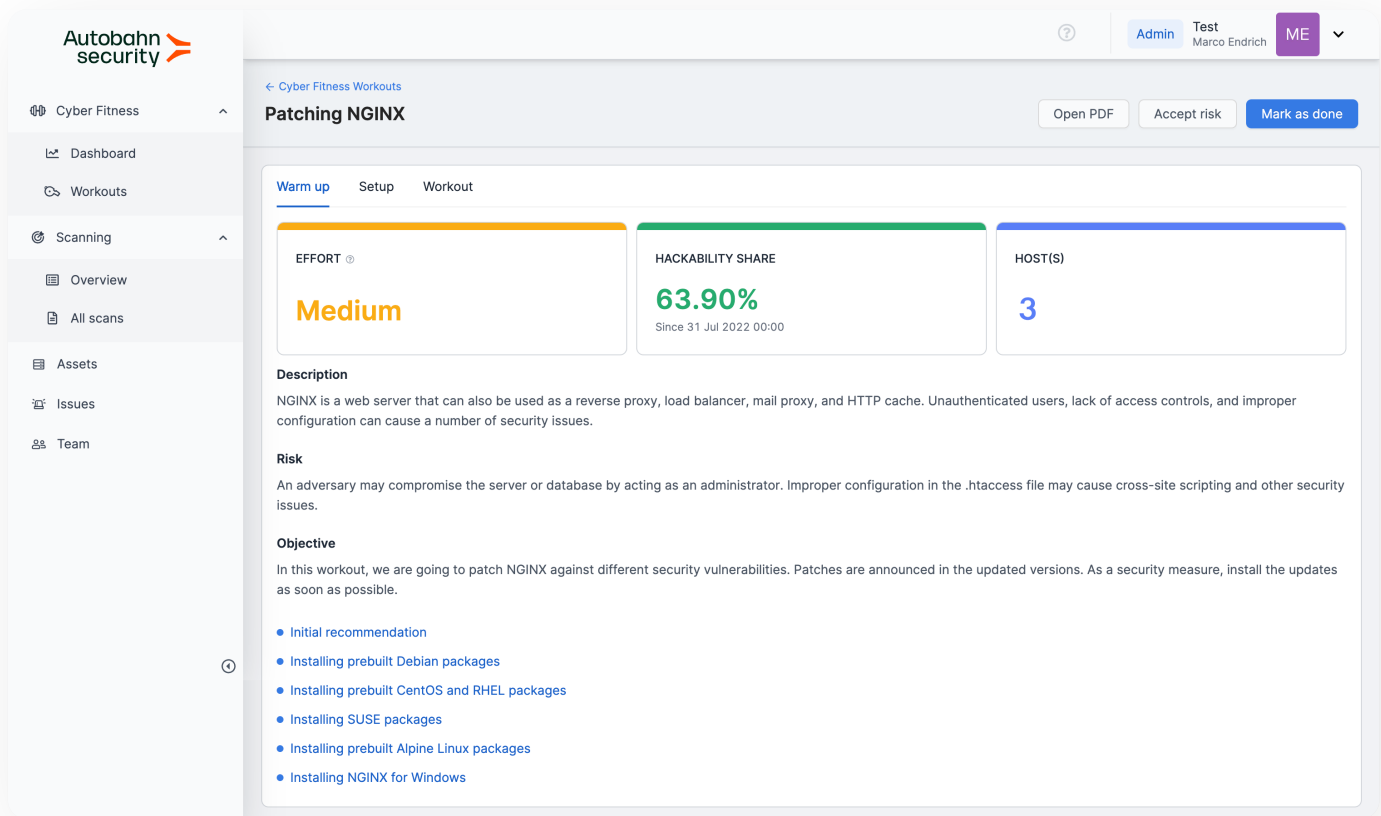
Although the range of hacker attacks is broad, you can often remediate multiple issues by installing a single patch or by tweaking a few settings to harden your system. Autobahn Security's signature Cyber Fitness Workouts explain how to do just that: which vital specific steps should be taken to make your organization more secure.

To illustrate, a patching workout often contains a step on where to get the latest stable software version. Besides, the workout might also tell you which system requirements to consider during the update or how to do a backup. In addition, the workout sheds light on how to automate updates or roll some of them back and tells you in what order to update specific components.
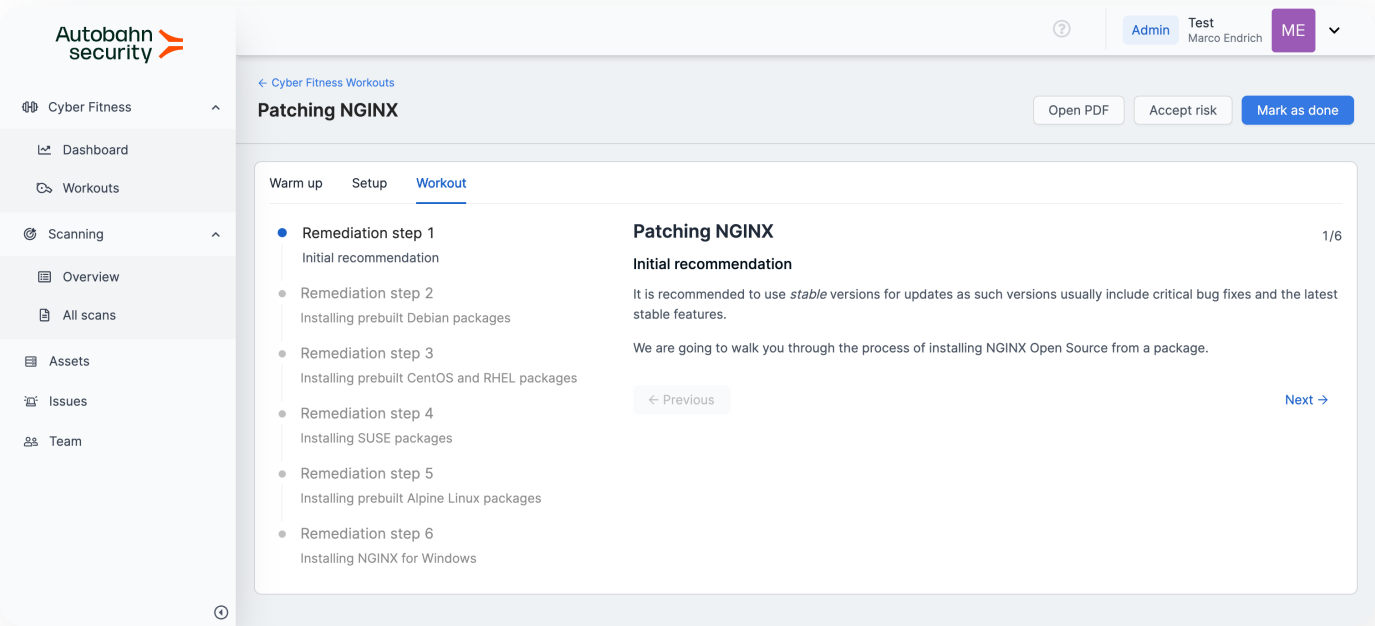
Figure 3. Example of the steps included in a Cyber Fitness Workout in the Autobahn platform. They are detailed and can be applied by non-IT security experts.

Your IT team will love it: armed with the necessary fixes, they only need to apply the provided solutions. And they can also send a ticket to Jira for tracking remediation progress. Each cyber fitness workout you take reduces your Hackability score and brings you closer to an ideal security posture.
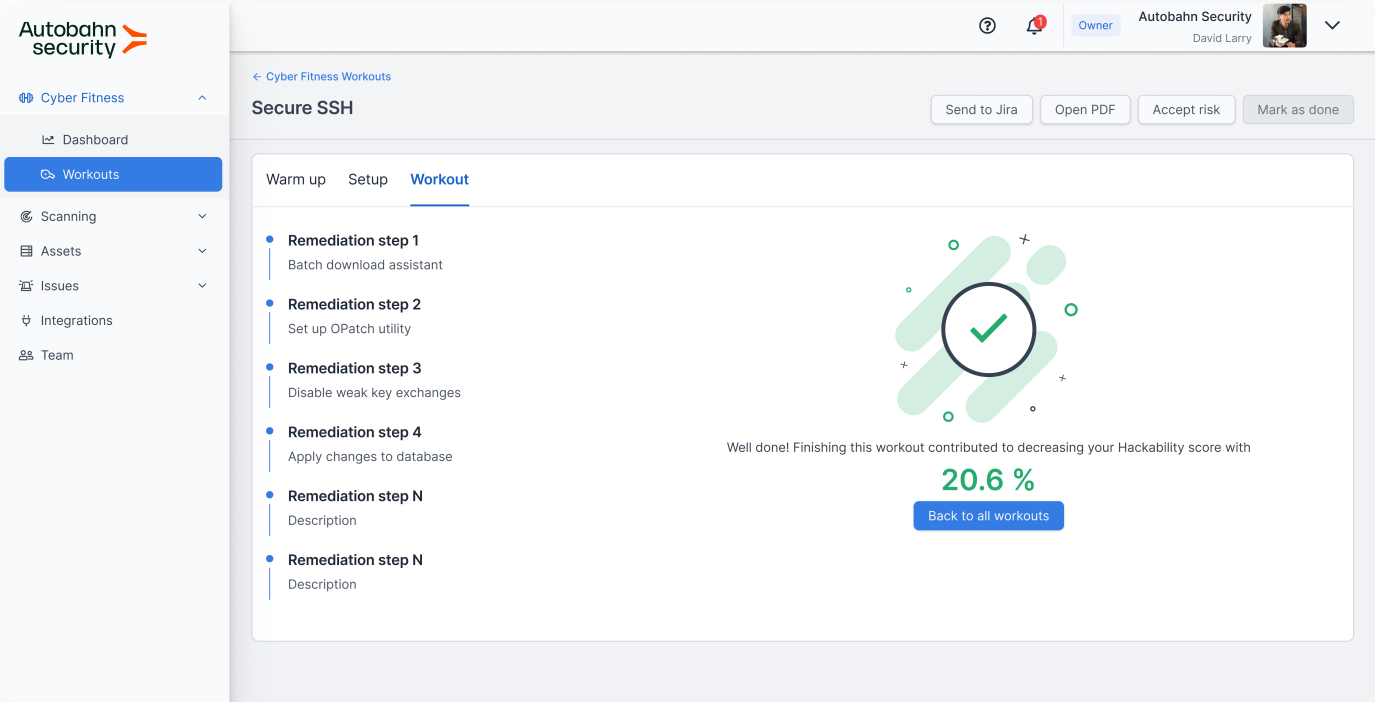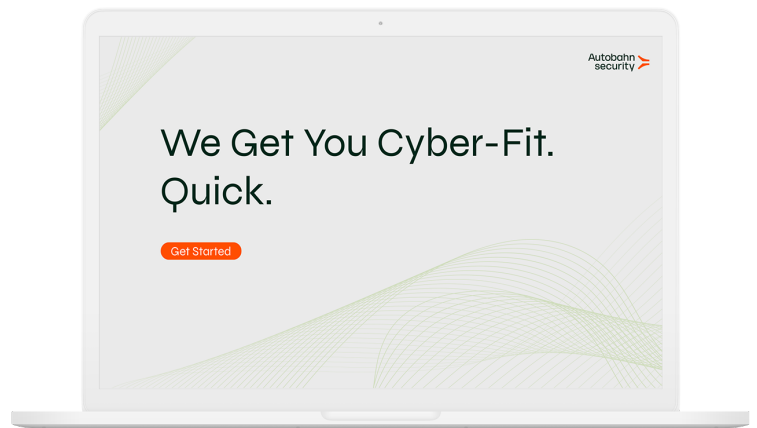

Figure 4. Example of a completed Cyber Fitness Workout in the Autobahn platform.

How you get started and what you can expect from us within just 1 week

- Understand your issue remediation process and pain points

- Walk through the key aspects of the platform

- Set up scans

- Evaluate scan results

We Get You Cyber-Fit. Quick.

Get Started

Request a free expert discussion right now

We evaluate your individual challenges, schedule a demo session, provide an overview of our value process, and discuss potential milestones and next steps.

Talk to our team to see how Autobahn Security can make you cyber-fit

Talk to us ⟶

Autobahn security