NORDIC DEFENDER

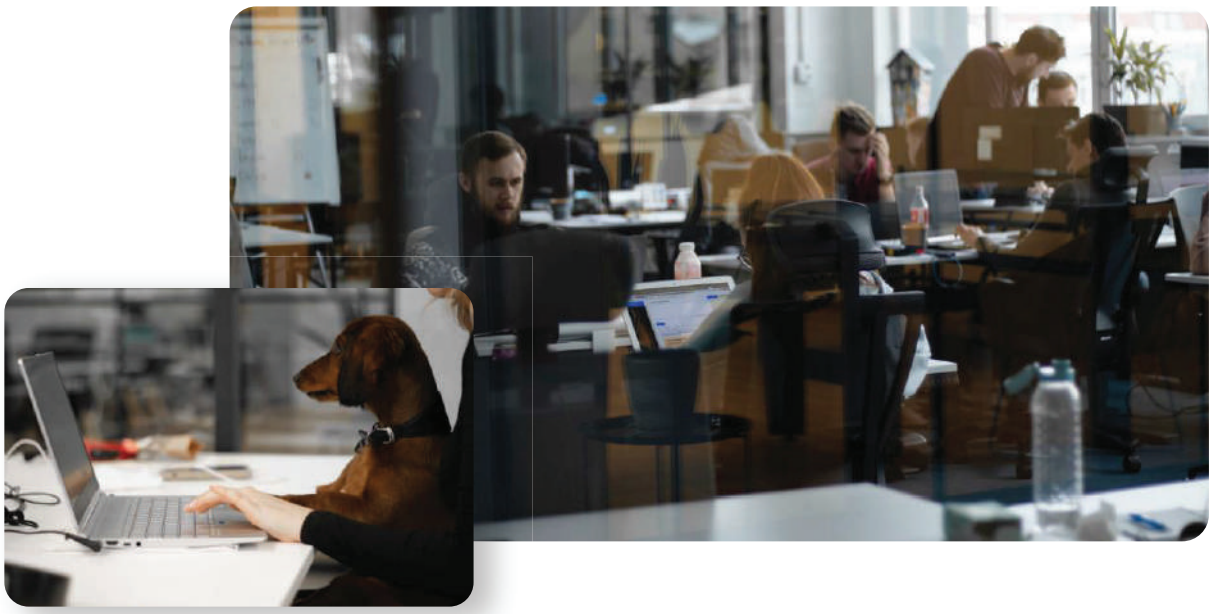
Modern Security Solutions Provider

Penetration Testing Buyer's Guide

Table of Content

Nordic Defender AB

Nordic Defender AB was founded in 2019 as the first crowd-powered managed security solution provider in Gothenburg, Sweden by a group of senior cybersecurity specialists to address cyber world issues including skill and talent gaps, complexity of security, and the lack of centralized security solutions.



For us, this isn't a job; it is a lifestyle, and this lifestyle has led to some of the best work on the market! We take pride in the fact that we are the first company in our industry to have created a crowd-powered MSSP that brings together offensive and defensive cybersecurity solutions.

Our Clients

zefec · VEIDEC · Stratsys · PROPLATE · esportal
reFitness · QUICKCHANNEL · PRAKTIKERTJÄNST · ADNAVEM
outnorth · Hertz · LeadPilot · Allevi
clavister · NOW INTERACT · EPULZE · ABILIA
GÖTEBORGS HAMN · KALIXKOMMUN · AQUA ROBUR · Workspace

Introduction

Safety and security have always been subject to heated debates and controversies. With the progress made in the field of cybersecurity, vicious attackers have sharpened their techniques as well. The cyber realm has never been faced with such an enormous threat landscape as it is now.

Of course, there is a way out, and it is called Pentest.

Note that science's improvements have proved to be a double-edged sword. Think of fire as an example; you can cook a well-done steak—please don't! Or you can burn a house down with it—again, please don't! Technology is no different. The progress in technology has given us many different tools and features, as well as fabulous security strategies and techniques. However, there is nothing without a downside.

What Is Pentest?

In simple terms, penetration testing, commonly referred to as Pentest, is simulated hacking into a system with permission from its owner—basically, an authorized, controlled cyberattack.

The only thing that can stop hackers is encountering them with a hacker's mindset. Hackers are the only ones that can stop their kind.

You have always heard that knowledge is power. We agree and disagree.

We consider knowledge as a prerequisite to power. If you intend to be powerful, you should have the underlying knowledge of who you are, where you are standing, and what your strengths and weaknesses are, and then use this knowledge and act on it. This is a surefire way to succeed.

Well, Nordic Defender Pentest gives you:

- insight into your systems' security status and your weak spots,
- solutions and resources for fixing the security issues you have,
- quick, easy integration for you to delegate the needed tasks directly to the related internal team,
- overall real-time monitoring of the found bugs with their severity level and those that have been fixed,
- and complete control over your budget and resource management.

With Pentest, you know where you stand, and you can decide to act on it and enhance your status. You can patch those weaknesses before a vicious hacker decides to attack you.

How Many Types of Pentesting Providers Are There?

Well, there are three main types of pentesting providers on the market: traditional consultancies, crowd-powered cybersecurity platforms, and Pentest as a Service (PTaaS). They are different with one another in terms of sourcing method, vetting procedure, and pentester-client connection.
However, Nordic Defender Next-Gen Pentest as a Service (PTaaS) changed the whole game using its innovative idea to provide the benefits of both crowd-powered cybersecurity platforms and the Pentest as a Service (PTaaS).

Traditional Consultancies

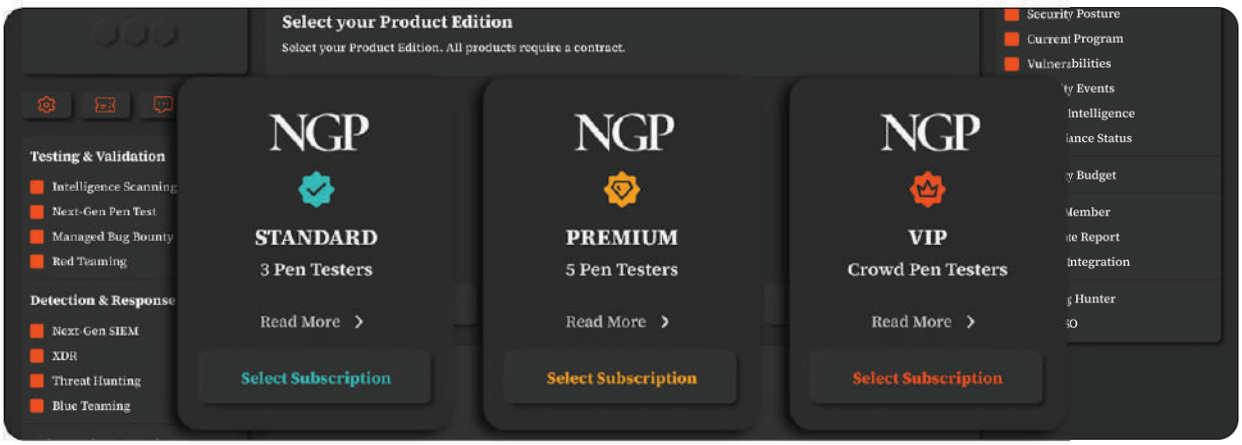
In traditional penetration testing, the client company hires an ethical hacker for the pentesting project. The high price, inefficiency compared to other models, and slow workflow of traditional pentesting make it the least likeable option on this list.

Crowd-Powered Cybersecurity Platforms

Crowd-powered cybersecurity platforms give the client company access to the pool that is filled with the knowledge, talent, and expertise of the crowd—a community of thousands of ethical hackers, divided into groups of different tiers ranging from unvetted to highly vetted. This enables the client company to access pentesters that are familiar with the intended industry.

Pentest as a Service (PTaaS)

Pentest as a Service (PTaaS) is one of latest penetration testing models. They take vetting processes more seriously, are more affordable and time-efficient, and offer SaaS platforms that prepare the client companies to take care of everything more productively.



Next-Gen Pentest as a Service (PTaaS)

Innovated by Nordic Defender, Next-Gen Pentest as a Service (PTaaS) not only is a mixture of the two models above, but it also offers more. Next-Gen Pentest as a Service (PTaaS) empowers the client company to access an exceptional pool of talented ethical hackers and get the pentest done at a higher speed and with significant precision. All the processes are managed by the dedicated technical account manager, communication between project managers, hackers and the client is direct and effective, and moderators will validate the bugs and remediations to ensure optimal results.

Nordic Defender Next-Gen Pentest as a Service (PTaaS) ROI

Nordic Defender Next-Gen Pentest as a Service (PTaaS) cybersecurity solution provides the client companies with a significant edge over other types of penetration testing solutions in terms of ROSI (Return on Security Investment). This basically means that Nordic Defender empowers businesses to gain better, more accurate results while keeping their budget intact.
Imagine a web application that needs 120 hours of pentesting. Using the traditional penetration testing approach, the client company will need to pay around €27,600 on average to get the job done; however, Nordic Defender Next-Gen Pentest as a Service (PTaaS) enables them to save €9,600 and invest just around €18,000 to achieve tremendously more benefits in less time.

Read the full Nordic Defender Next-Gen Pentest as a Service (PTaaS) ROI guide to gain a deeper insight into how Nordic Defender manages to outperform traditional consultancies.

Some features you will gain:

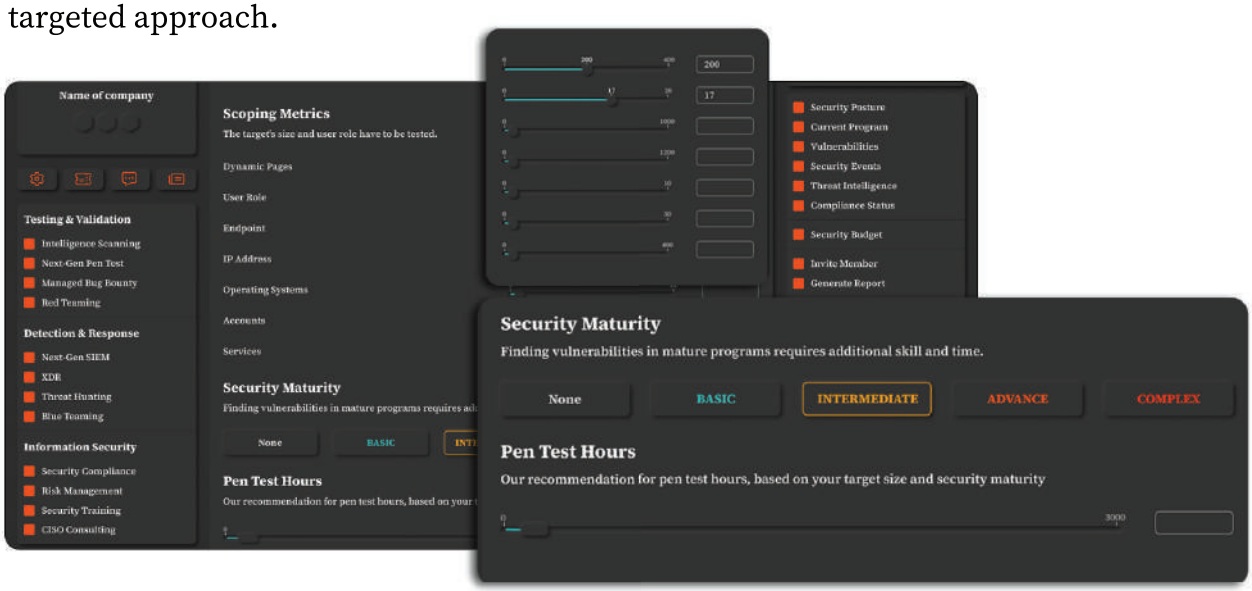
- Full coverage of customer security certification
- Centralized, easy-to-use security control panel
- Team collaboration and task management availability through the platform
- Total digital transformation of testing activities
- Covering a large range of targets in one test

Who Should Use Pentest?

Anybody whose business includes any kind of web/mobile applications, networks, APIs, IoT, or other digital assets needs Pentest. Whether you are a small business, a mid-sized organization, or a megacorporation, you need to know where you stand in terms of security.
If you have any kind of online services, you are a potential target for getting hacked.

Pentest Use Cases

It is of significant value to know the reason you want to conduct a pentest. Having an explicit purpose enables you to determine what type of pentest you want to conduct and whether you want it all at once on all of your assets or you want to go for a more targeted approach.



Compliance Testing

Nowadays, many industries require some cybersecurity regulations to be met so that valuable data can be protected. One instance is the HIPAA compliance which has been extended for healthcare industries. Many regulations even explicitly need pentesting to ensure the business's robust cybersecurity status. The Payment Card Industry Data Security Standard (PCI DSS) needs a thorough implementation of a pentest program in one of its requirements. Continuous implementation of pentests empower you to stay one step ahead all the time. Nordic Defender Next-Gen Pentest as a Service (PTaaS) empowers you to meet compliance requirements such as SOC 2, PCI-DSS, ISO 27001, NIST 800-53, HIPAA, and CREST.

Customer Requests

Your client or a third-party might need to know that you are a secure organization in the cyber realm and that their data is in safe hands. Especially when it comes to data related to industries such as healthcare, finance exchanges, or banking systems, there are many concerns to consider. Nobody wants to have their medical information or their credit card numbers, passcodes, dates, and CVV numbers leaked into the hands of a group of malicious attackers. You can conduct Nordic Defender Next-Gen Pentest as a Service (PTaaS) to ensure your clients and partners that their data is safe and ease their minds.

Elevating Your Cybersecurity Posture

Cybersecurity is not all about satisfying others. It is not just about meeting compliances and customer requests. The most important part of cybersecurity is making sure your assets are as safe as possible to ensure data safety, brand reputation, and business continuity.

Pentest Integration Into Software Development Life Cycle

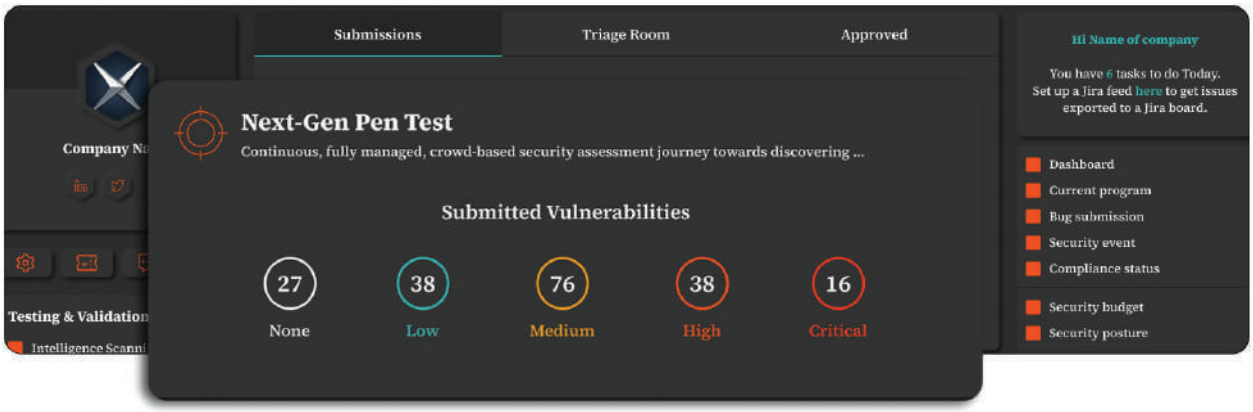
Knowing that your systems were secure at some point but dealing with many vulnerabilities right now is not the best state to be in. You always want to be one step ahead of cyber criminals and you want your online assets to be secure at all times. This is especially true when we are talking about software development. In the software development life cycle, assets will change over time. Code will be modified everyday and several open-source or commercial components might be used. This is where performing a continuous Pentest and integrating it into the Software Development Life Cycle helps you ensure that you are secure in every step of the way.

Re-Testing

There are times when you want to validate that the remediation steps you took have fixed the problem. This is when you should conduct a retest to ensure that the proficiency of both the pentest and the actions you took to mitigate the issue. With Nordic Defender Next-Gen Pentest as a Service (PTaaS), you can simply request for a retest after your development department has fixed the issues, vulnerabilities, or misconfigurations.

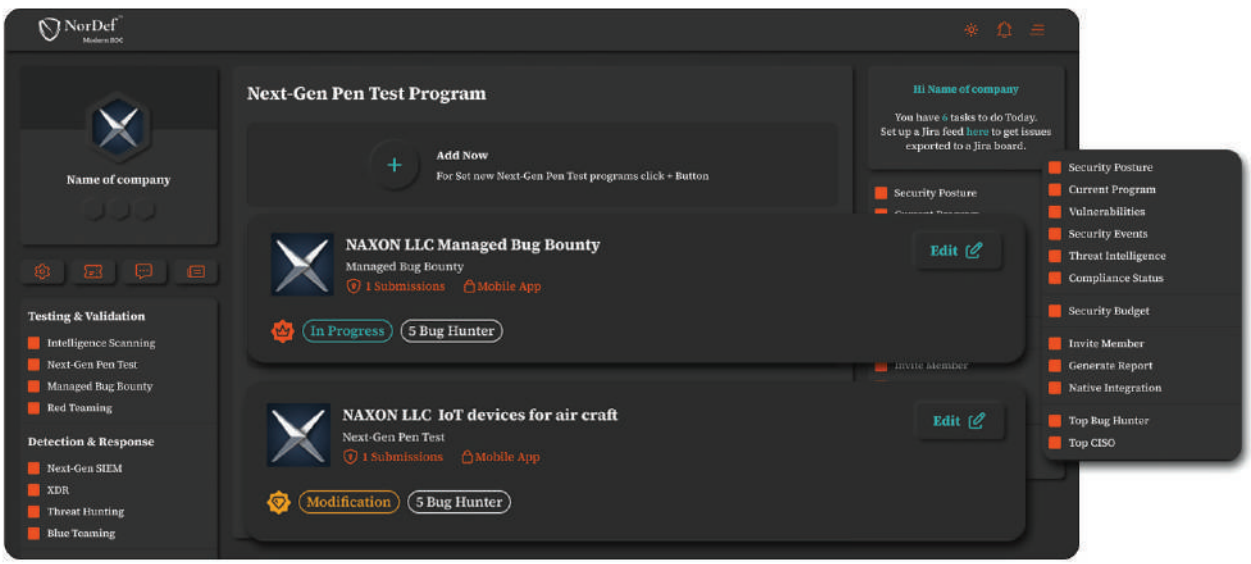
New Release Testing

As mentioned earlier, software is always being developed and released. This can be seen as a problem in terms of cybersecurity posture. The reason is that you want every release of your software to be as secure as possible so that both your business and your customers are safe. New features, updates, bug fixes, etc. can be part of a new software release. With new release testing, you can make sure that you are delivering your newest release as secure as possible.



Category-Specific Testing

Shrink down your testing scope and interest to a specific testing category, vulnerability type or target sub-devision. You can test a single vulnerability such as Log4j or a small part of your asset to ensure that you are safe. Conduct single OWASP category testing on your web, mobile, or API asset to confirm its security.



How Does Pentest Work?

There are many different methods of Pentest out there, and depending on the selected method, there will be some stages to it. You do not need to be afraid of technical details if you are not a technical person. Nordic Defender's team will assemble everything according to your needs and detailed technical assessments. Keep reading to understand how it works in more detail.

Stages

Information Gathering

For the first step, our ethical hacker will conduct research and will gain as much information and intelligence as possible about the target and how it works.

Hands-on Testing

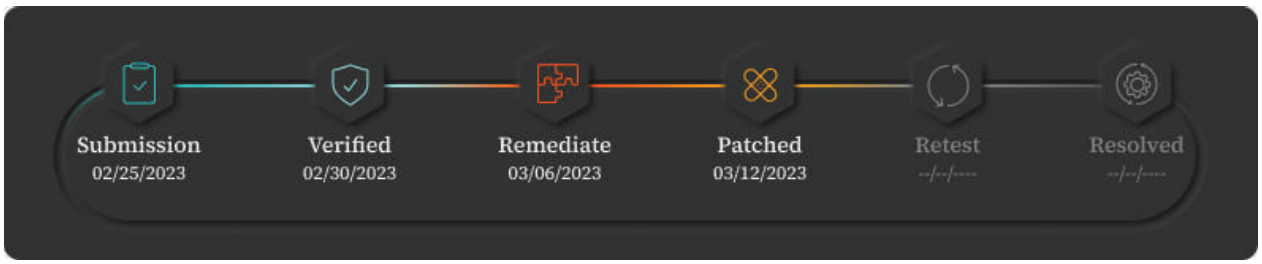
The ethical hacker will check the attack possibility on your target using different tools and techniques. They will test all testing scenarios to show how they could damage you if they were a malicious attacker. This will provide you with insight into the type and scale of damage, but they will never perform the actual damage. They will also make sure to cover all testing best practices and checklists.

Reporting

Upon the completion of each testing scenario, a comprehensive report is written and delivered to the customer, including test target information, found vulnerabilities with proof in written version and supportive PoC, and accurate remediation recommendations.

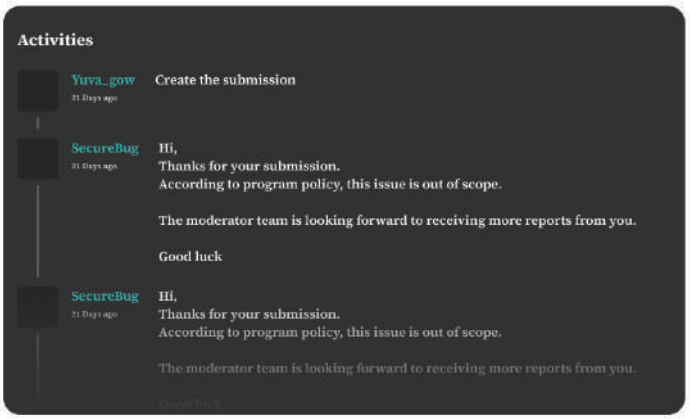
Nordic Defender Vulnerability Management Life Cycle

Nordic Defender Next-Gen Pentest as a Service (PTaaS) has a foolproof life cycle for its vulnerability management. This life cycle consists of 6 stages about which we will talk about right now.



1. Bug Submission

The security researchers who have been assigned to the project will submit bugs, vulnerabilities, or misconfigurations of various types and severities in the platform's dashboard.



2. Bug Verification

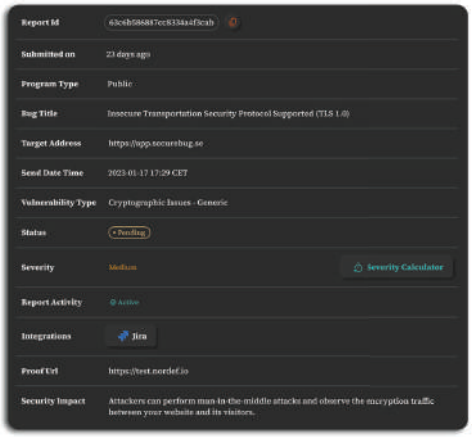
Next, security engineers verify the findings and their severity. They make sure that there are no duplicates and out-of-scope issues and improve the report quality and precision. Moreover, the security engineers check the proof of concept (PoC)—in the form of pictures and videos—and recreation steps.

3. Remediation

The submissions and the remediation provided in the previous steps which is accessible through the platform can be integrated into the Jira workflow. This enables the developers to start taking care of the issues and start fixing the vulnerabilities and misconfigurations that were found.

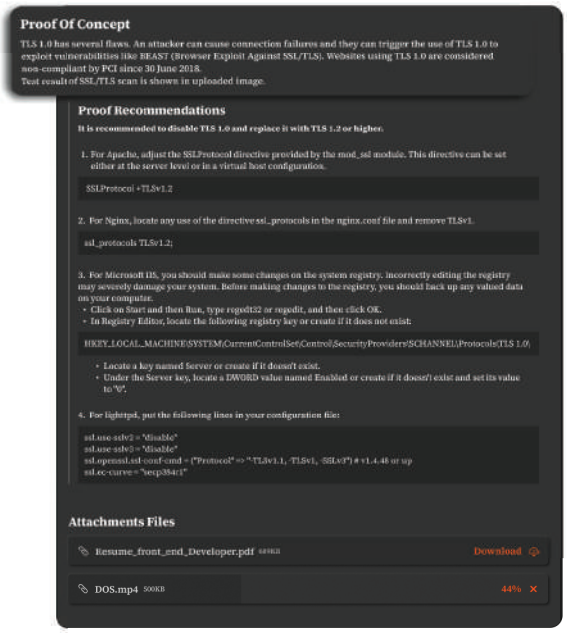
4. Patching

Afterward, the customer's development team will work on fixing the bugs and ensuring that all the validated submissions are mitigated. They are welcome to ask their questions or share their doubts with the security researchers and engineers and they will come back with the solution as soon as possible.



5. Retesting

Then, a retesting will be conducted on the assets by the customer's request to ensure that everything is successfuly patched and ready to be securely used by end users.



6. Resolving

Finally, after making sure that the submission is fully mitigated, the report is marked as resolved, meaning that the patching is done effectively.

Experience Security with Nordic Defender

Founded in 2020 in Gothenburg, Sweden, Nordic Defender AB is the first crowd-powered modern cybersecurity solution provider in the Nordic region. Being exceedingly customer-centric, Nordic Defender tailors its solutions to all types of industries, especially online and SaaS-model businesses so that they can implement security compliances and benefit from application security, real-time monitoring, and SOC solutions. Many companies and organizations in different industries—such as governmental, healthcare, environmental, cryptocurrency, and even cybersecurity itself—use the comprehensive solutions Nordic Defender provides to ensure a robust cybersecurity posture and business continuity.
Start using Nordic Defender right now and stay safe in the cyber realm!

Are you ready to enhance your security measures?

Nordic Defender is the only crowd-powered, fully-managed MSSP, where combined offensive and defensive solutions are employed to expose blind spots in your attack surface before attackers get the chance to take advantage.

Contact us! We will lead the way

Contact us to get started!

sales@nordicdefender.com

Learn More at **www.NordicDefender.com**

Get in touch with us:

NORDIC DEFENDER

Modern Security Solutions Provider

Nordic Defender AB is a swedish limited company with a registered office in in Gothenburg Sweden , Södra Vägen 2 , 412 56 SE -Org.nr: 559201 - 3030 that provides managed offensive and defensive security solutions