NetCaptain

NetCaptain
A brand of CyberAnt

WHAT IS NETCAPTAIN

Every day, new security vulnerabilities in software are discovered. Keeping up with this continuous stream of new vulnerabilities requires a lot of time and expertise.

NetCaptain has automated this process and is now one of the best vulnerability management tools in all of Europe. NetCaptain provides clear and understandable advice on how vulnerabilities can be resolved.

Compared to other vulnerability tools, NetCaptain scans many more times and is also very affordable.

NetCaptain features a Get Help function, which means that our cybersecurity experts are ready to answer all unanswered questions. NetCaptain can be installed by deploying either a physical or virtual appliance.

NETCAPTAIN KEEPS HACKERS OUT

Many cyberattacks are relatively easy to prevent. This is because hackers often exploit weaknesses in systems that are known and for which there is already a solution. However, it can be challenging to be sure that all systems are secure. How can you be certain that a security update has indeed fixed the problem? And are there no servers left out of the process?

WHAT SECURITY VULNERABILITIES EXIST?

Security scans are used to examine systems, network components, and web applications for security vulnerabilities. By addressing these vulnerabilities, the resilience against cyberattacks is increased, reducing the likelihood of a successful attack to a minimum.

UNDERSTANDABLE AND AFFORDABLE

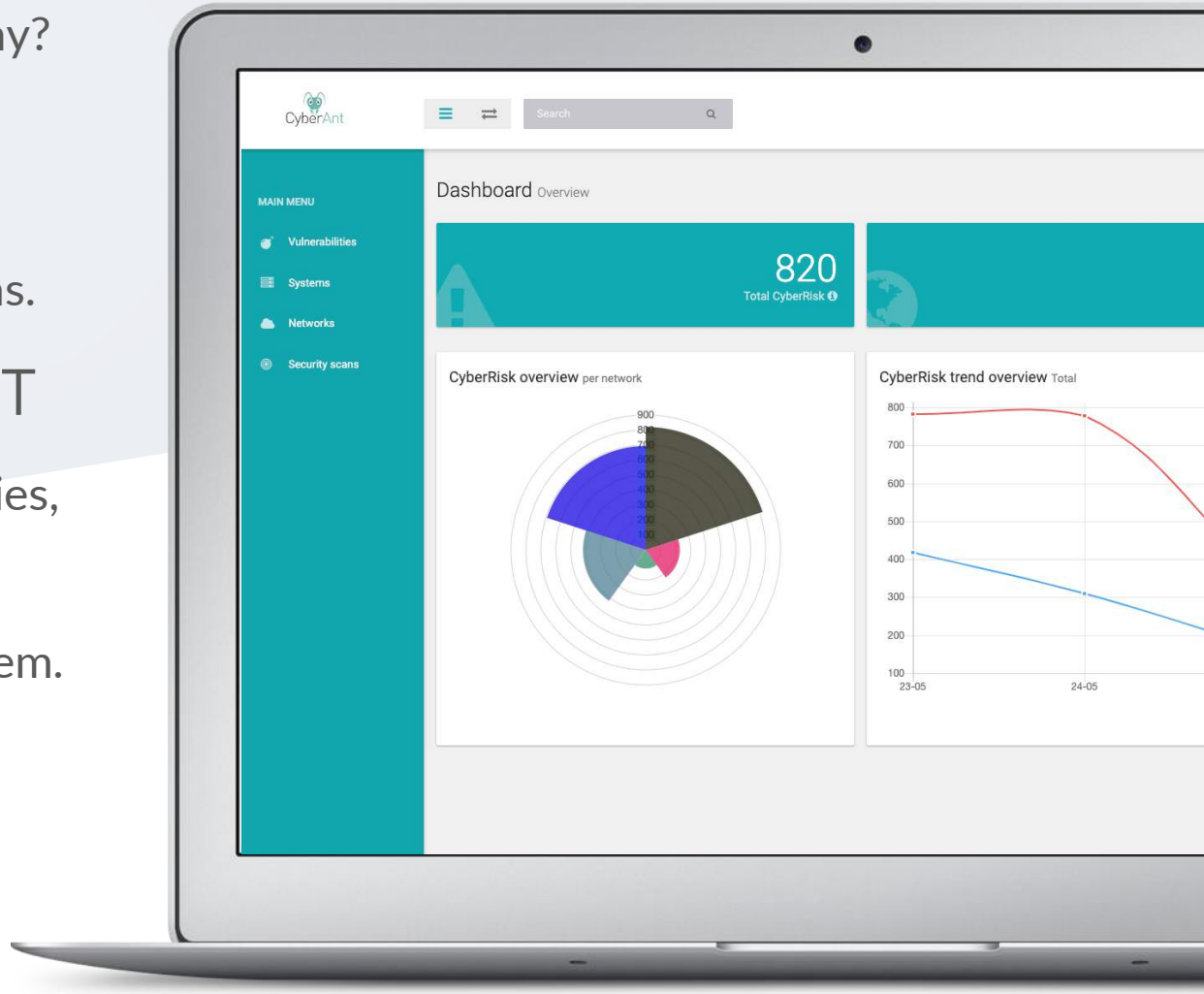
New vulnerabilities in software are discovered daily. Managing this continuous flow of new vulnerabilities requires a smart approach. This is known as Vulnerability Management. NetCaptain automates this process and provides clear and understandable advice.

CLEAR DASHBOARD

At a glance, you can see how you're doing.

Are we becoming more secure?
Where are the biggest risks in my company?
Which vulnerabilities need my immediate attention?

The NetCaptain dashboard is designed to provide instant answers to these questions.

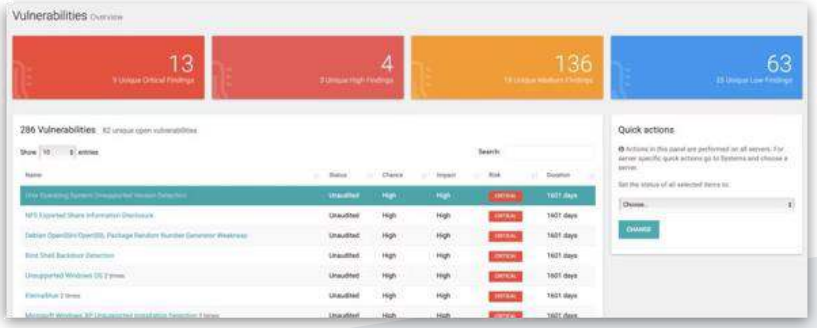


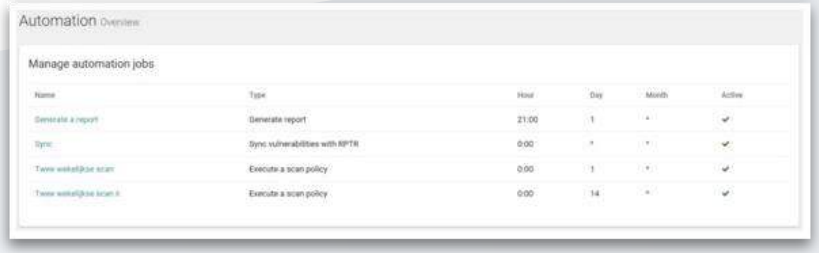
VULNERABILITY MANAGEMENT

NetCaptain neatly displays all vulnerabilities, groups similar ones automatically, tracks their history, and sends warnings if a vulnerability reappears abruptly on a system.

AUTOMATE THE PROCESS

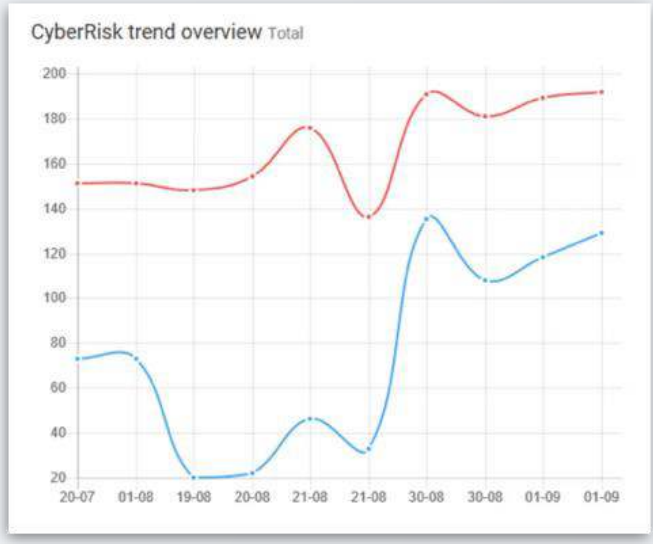
With NetCaptain, you can schedule when you want to perform scans. Workstations can be scanned during working hours, network equipment at night, and Windows servers after Patch Tuesday.





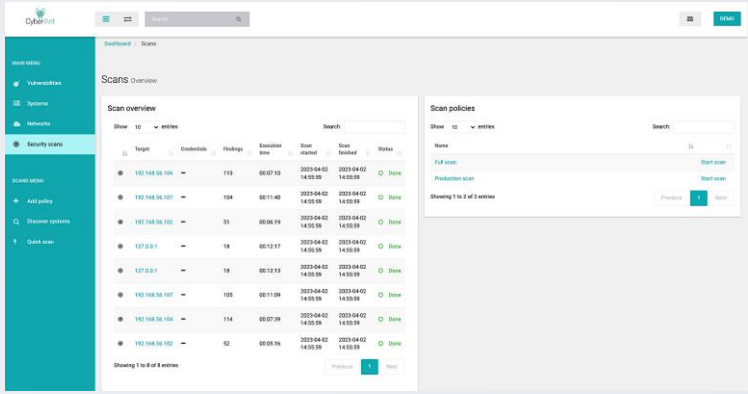
TREND OVERVIEW

In the trend overview, you can monitor your network's security over time, tracking vulnerabilities and the automated CyberRisk score. This helps you closely follow your vulnerability management progress, with the score factoring in severity, system importance, and internet accessibility.



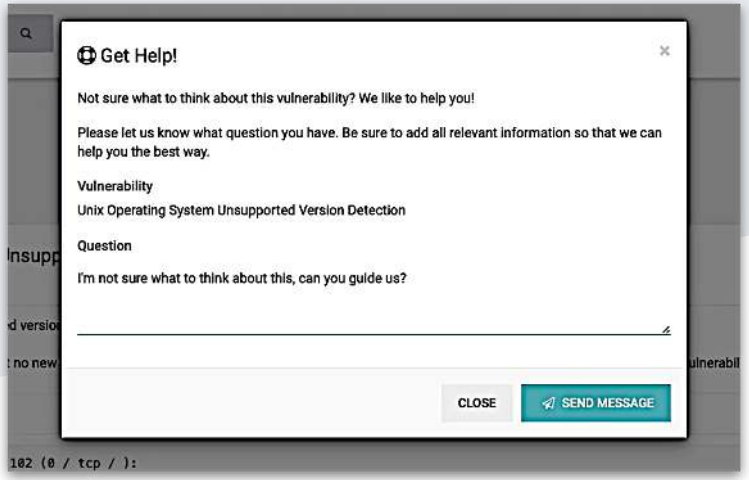
SCAN MANAGEMENT

In the scan overview, you can monitor your scanning activities, view detected vulnerabilities, check scan dates, credential usage, and any errors. This section also allows you to manage discovery scans, helping you identify new network systems and avoid overlooking forgotten ones.



HELP IS ALWAYS CLOSE BY

The Get Help feature lets you ask our ethical hackers directly from your dashboard about vulnerabilities, granting you access to both tools and expertise. With NetCaptain, you're never alone. Get Help is available for Professional and Enterprise customers.



WHAT DOES NETCAPTAIN CHECK

NetCaptain is capable of detecting vulnerabilities within servers, databases, IoT devices (such as cameras and printers), web applications, and workstations. It is also possible to use NetCaptain within cloud environments.

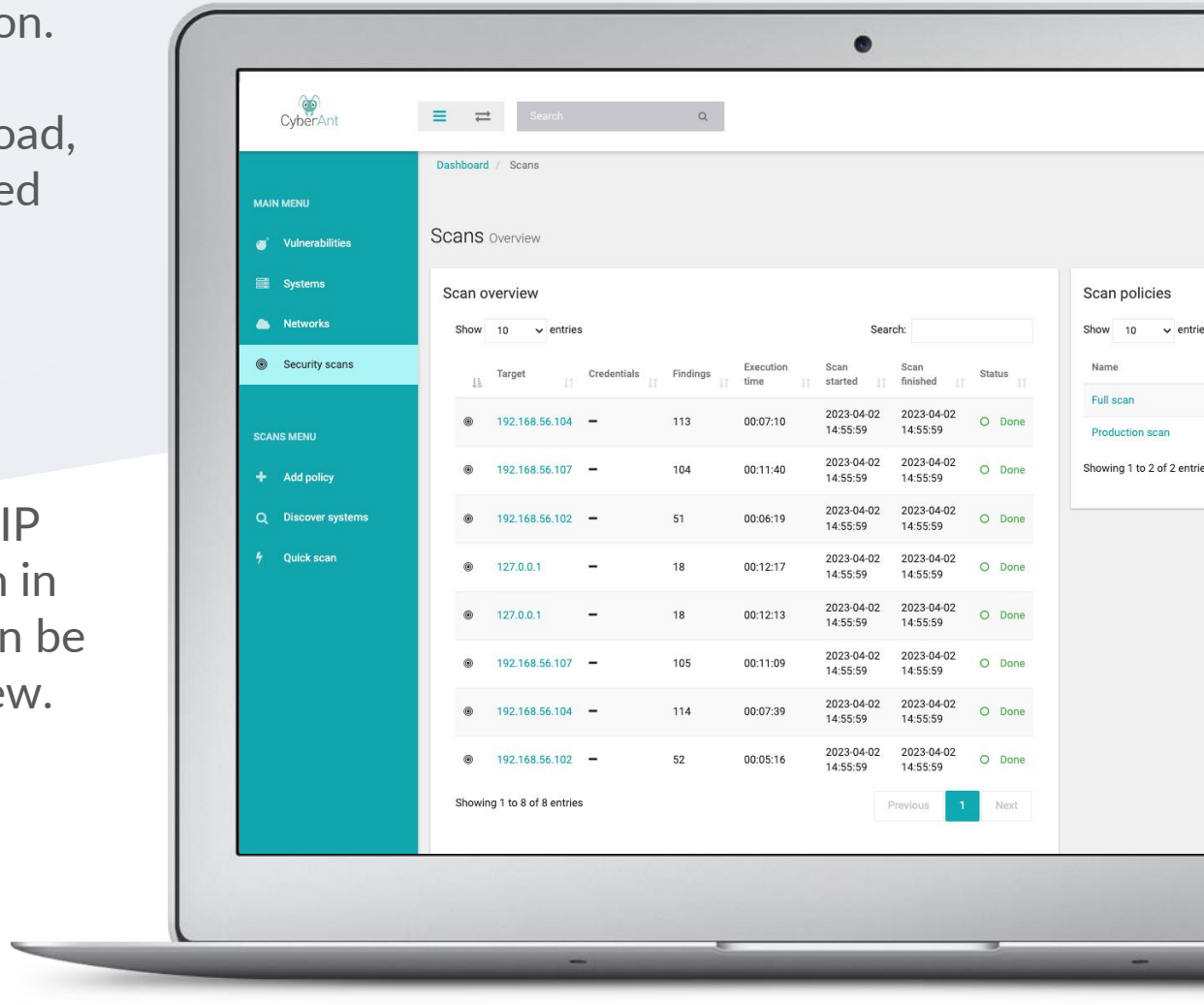
NetCaptain scans everything in the network, even unknown or forgotten devices, enhancing network security comprehensively

HOW MANY SYSTEMS CAN NETCAPTAIN SCAN

NetCaptain can scan all network systems, whether you're a large or small organization. For very large networks, multiple scan engines are used. To avoid network overload, scans can be scheduled at night or confined to specific segments.

NetCaptain comes with a base number of systems that you can scan in the license.

A system is also referred to as a target or IP address. With the included discovery scan in NetCaptain, all systems in the network can be found. This way, all systems come into view.



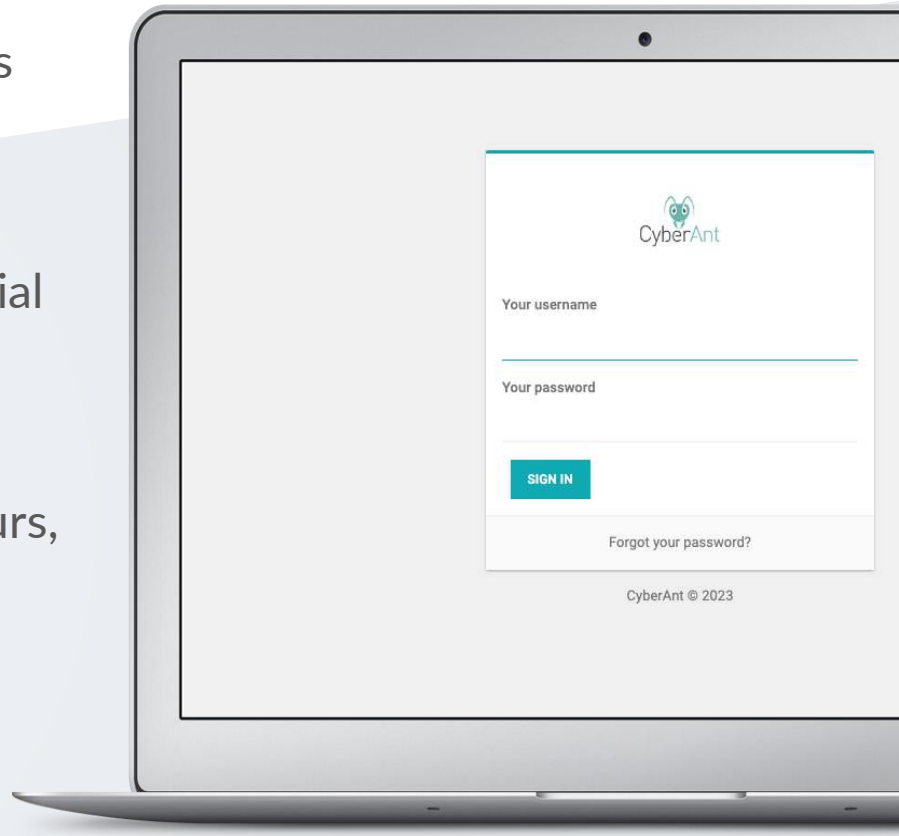
HOW TO IMPLEMENT NETCAPTAIN

The process begins with an intake by our technical specialists to evaluate the network's situation.

Once the system count and need for multiple scan engines are determined, an ISO file is provided for NetCaptain installation and activation using a license code.

Our specialists oversee correct installation, assist with initial scans and policy setup.

NetCaptain's user-friendly design eliminates the need for special training. On average, installation takes about 3 hours, with exceptions occasionally requiring additional time



CONTACT

CyberAnt B.V.
Marconiweg 1
3899 BR Zeewolde
The Netherlands
Email: info@cyberant.com
Phone: +31 85 047 1590

NetCaptain
A brand of CyberAnt