NetCaptain

NetCaptain
A brand of CyberAnt

WAT IS NETCAPTAIN

Elke dag worden er nieuwe beveiligingskwetsbaarheden in software ontdekt. Het bijhouden van deze continue stroom van nieuwe kwetsbaarheden vereist veel tijd en expertise.

NetCaptain heeft dit proces geautomatiseerd en is nu een van de beste vulnerability management tools in heel Europa. NetCaptain biedt duidelijk en begrijpelijk advies over hoe kwetsbaarheden kunnen worden opgelost.

Vergeleken met andere hulpmiddelen voor kwetsbaarheden scant NetCaptain vele malen meer en is het ook zeer betaalbaar.

NetCaptain heeft een Get Help functie, wat betekent dat onze cybersecurity-experts klaar staan om alle onbeantwoorde vragen te beantwoorden. NetCaptain kan worden geïnstalleerd door het inzetten van een fysieke of virtuele appliance.

NETCAPTAIN HOUDT HACKERS BUITEN

Veel cyberaanvallen zijn relatief gemakkelijk te voorkomen. Dit komt omdat hackers vaak bekende zwakke plekken in systemen uitbuiten waarvoor al een oplossing bestaat. Echter, het kan een uitdaging zijn om er zeker van te zijn dat alle systemen veilig zijn. Hoe weet je zeker dat een beveiligingsupdate het probleem daadwerkelijk heeft opgelost? En zijn er geen servers overgeslagen in het proces?

WELKE BEVEILIGINGSKWETSBAARHEDEN BESTAAN ER?

Beveiligingsscans worden gebruikt om systemen, netwerkcomponenten en webapplicaties te onderzoeken op beveiligingskwetsbaarheden. Door deze kwetsbaarheden aan te pakken, wordt de weerstand tegen cyberaanvallen verhoogd en de kans op een succesvolle aanval tot een minimum beperkt.

BEGRIJPELIJK EN BETAALBAAR

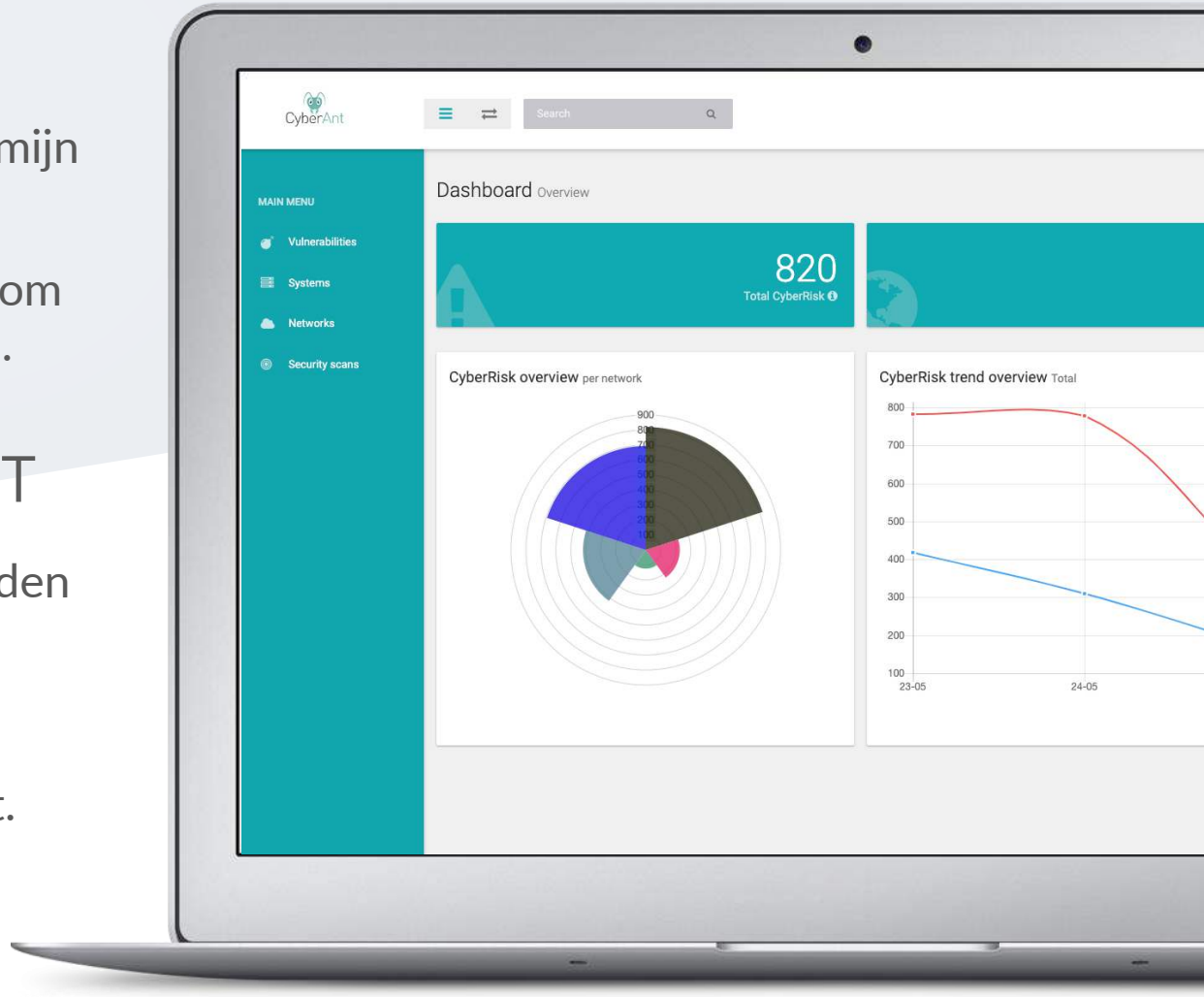
Nieuwe kwetsbaarheden in software worden dagelijks ontdekt. Het beheren van deze constante stroom van nieuwe kwetsbaarheden vereist een slimme aanpak. Dit staat bekend als Vulnerability Management. NetCaptain automatiseert dit proces en biedt duidelijke en begrijpelijke adviezen.

OVERZICHTELIJK DASHBOARD

In één oogopslag inzicht in hoe het er voor staat.

Worden we veiliger?
Waar liggen de grootste risico's in mijn bedrijf? Welke kwetsbaarheden vereisen mijn directe aandacht?

Het NetCaptain-dashboard is ontworpen om direct antwoord te geven op deze vragen..

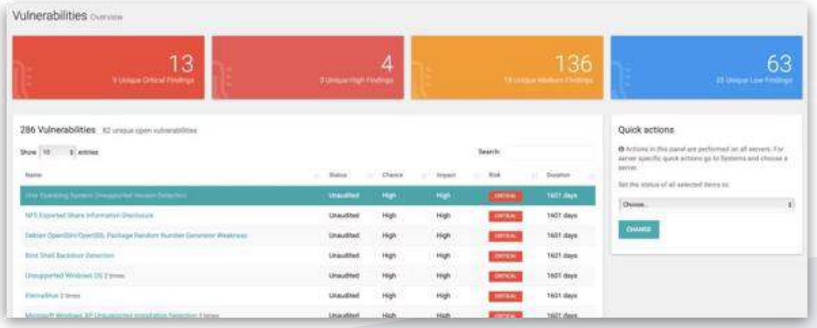


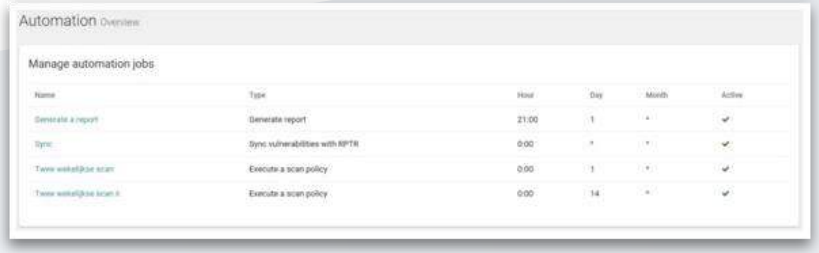
VULNERABILITY MANAGEMENT

NetCaptain geeft netjes alle kwetsbaarheden weer, groepeert soortgelijke automatisch, volgt de geschiedenis en stuurt waarschuwingen als een kwetsbaarheid plotseling weer op een systeem verschijnt.

AUTOMATISEER HET PROCES

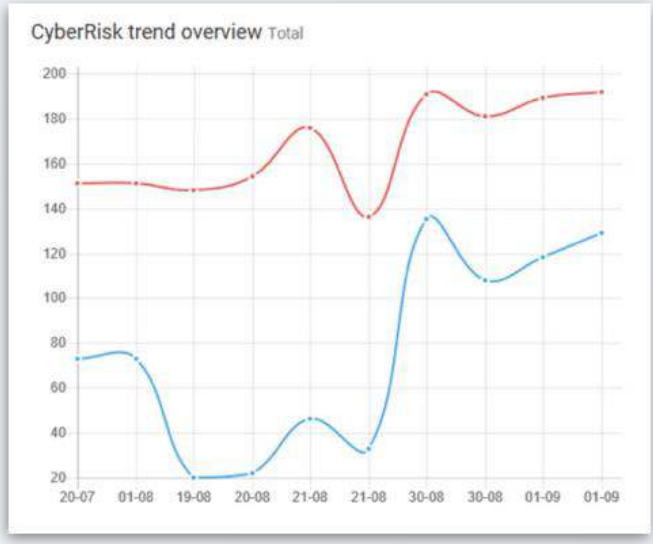
Met NetCaptain kun je plannen wanneer scans worden uitgevoerd. Werkstations kunnen tijdens kantooruren worden gescand, netwerkapparatuur 's nachts, en Windows-servers na Patch Tuesday.





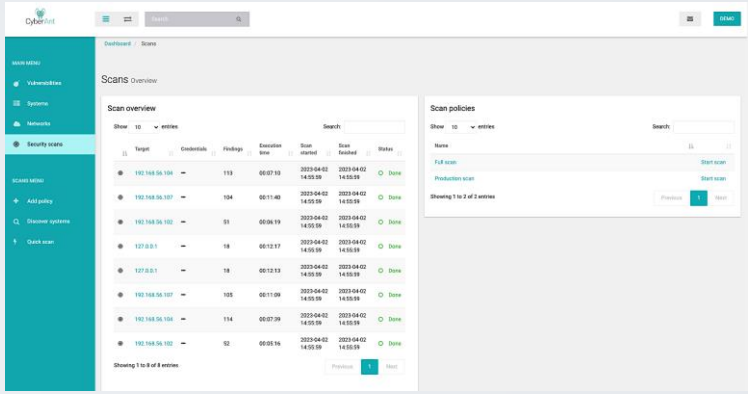
TREND OVERZICHT

In het trendoverzicht kunt is de beveiliging van het netwerk in de loop van de tijd monitoren, waarbij kwetsbaarheden en de geautomatiseerde CyberRisk-score worden bijgehouden. Dit helpt om de vooruitgang op het gebied van kwetsbaarheidsbeheer nauwlettend te volgen, waarbij de score rekening houdt met de ernst, het belang van het systeem en de internettoegankelijkheid.



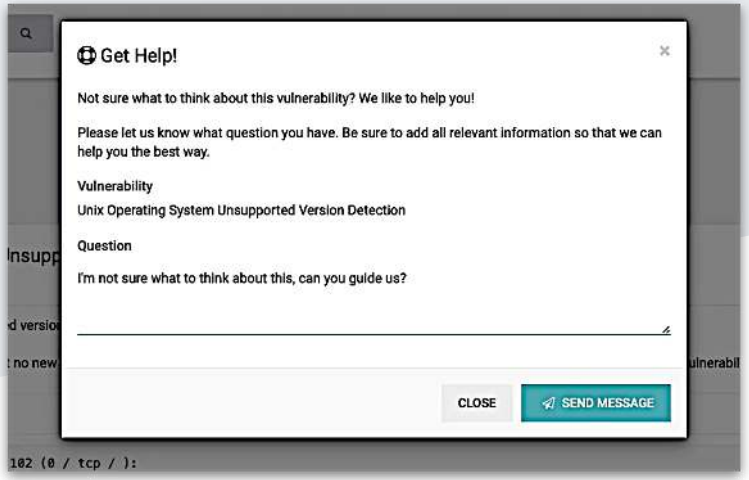
SCAN MANAGEMENT

In het scanoverzicht kun je de scanactiviteiten monitoren, gedetecteerde kwetsbaarheden bekijken, scandata controleren, het gebruik van inloggegevens en eventuele fouten. Dit onderdeel stelt je ook in staat om ontdekkingsscans te beheren, waardoor nieuwe netwerksystemen geïdentificeerd kunnen worden en voorkomt dat vergeten systemen over het hoofd gezien worden.



HULP IS ALTIJD DICHTBIJ

De functie Get Help stelt je in staat om direct vanuit het dashboard onze ethische hackers vragen te stellen over kwetsbaarheden, waarbij je toegang krijgt tot zowel tools als expertise. Met NetCaptain sta je er nooit alleen voor. Get Help is beschikbaar voor Professional en Enterprise klanten.



WAT CHECKT NETCAPTAIN

NetCaptain kan kwetsbaarheden detecteren in servers, databases, IoT-apparaten (zoals camera's en printers), webapplicaties en werkstations. Het is ook mogelijk om NetCaptain te gebruiken binnen Cloud omgevingen.

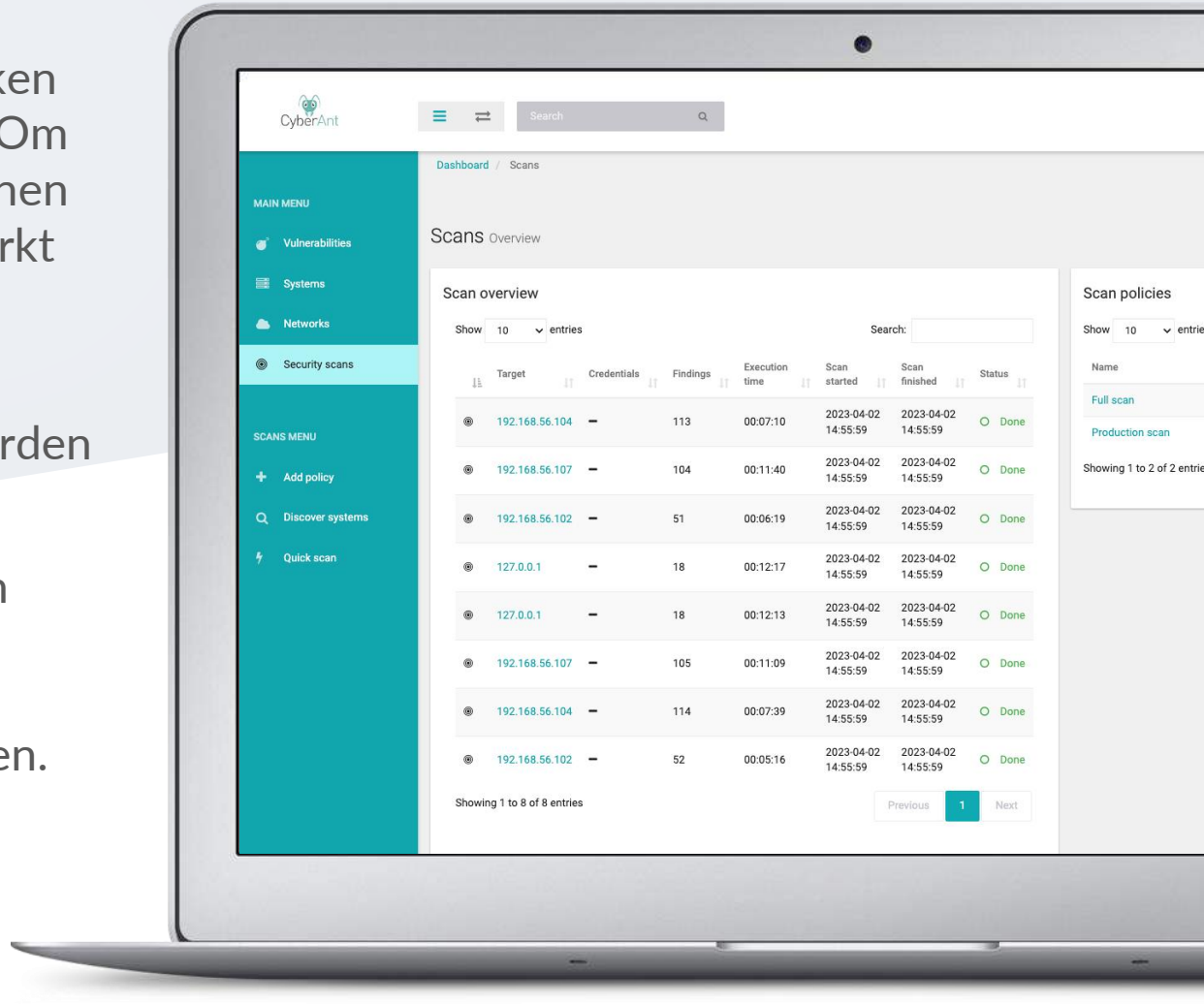
NetCaptain scant alles in het netwerk, zelfs onbekende of vergeten apparaten, en verbetert zo de netwerkbeveiliging op een alomvattende manier.

HOEVEEL SYSTEMEN KAN NETCAPTAIN SCANNEN

NetCaptain kan alle netwerksystemen scannen, of je nou een grote of kleine organisatie bent. Voor zeer grote netwerken worden meerdere scan engines gebruikt. Om netwerkoverbelasting te voorkomen, kunnen scans 's nachts worden ingepland of beperkt worden tot specifieke segmenten.

NetCaptain wordt geleverd met een basisaantal systemen dat gescand kan worden binnen de licentie.

Een systeem wordt ook aangeduid als een target of IP-adres. Met de bijgeleverde discovery scan in NetCaptain kunnen alle systemen in het netwerk worden gevonden. Op deze manier komen alle systemen in beeld.



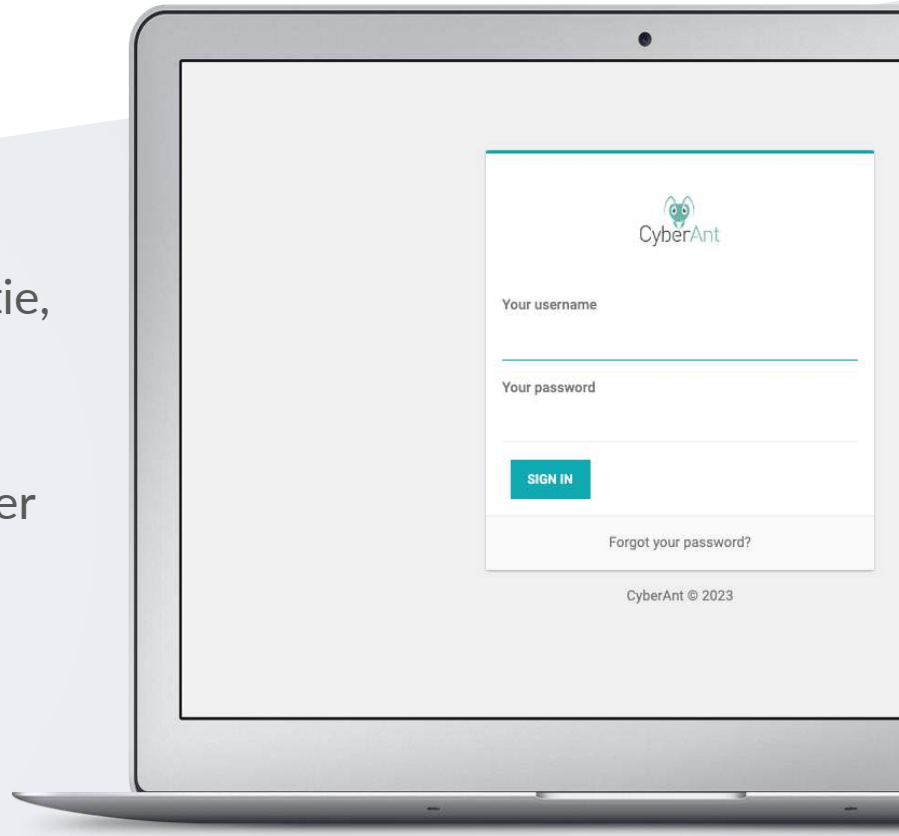
HOE NETCAPTAIN TE IMPLEMENTEREN

Het proces begint met een intake door onze technische specialisten om de situatie van het netwerk te evalueren.

Zodra het aantal systemen en de behoefte aan meerdere scan engines zijn vastgesteld, wordt een ISO-bestand verstrekt voor de installatie en activering van NetCaptain met behulp van een licentiecode.

Onze specialisten houden toezicht op de correcte installatie, helpen bij de initiële scans en het opzetten van beleid.

NetCaptain's gebruiksvriendelijke ontwerp maakt speciale training overbodig. Gemiddeld duurt de installatie ongeveer 3 uur, met uitzonderingen die soms extra tijd vereisen.



CONTACT

CyberAnt B.V.
Marconiweg 1
3899 BR Zeewolde

Email: info@cyberant.com
Phone: +31 85 047 1590

NetCaptain
A brand of CyberAnt