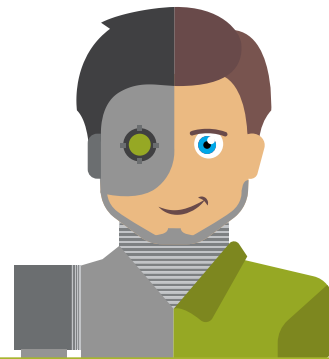


## Hybride vulnerability scanning door Marvin\_

### Ontmoet Marvin\_

Onze hybride dienst:  
half tool, half test specialist.



Een security test als momentopname is fijn, maar dagelijks inzicht is beter. Tussen de periodieke pentests ben je immers kwetsbaar. Daarnaast helpt dagelijks inzicht je compliant te blijven met bijvoorbeeld je ISO 27001-certificering of GDPR/AVG maatregelen. Bestaande scantools kunnen hier helpen, maar de scanresultaten zijn complex en zorgen veelal voor extra werk omdat de resultaten moeten worden bekeken en geanalyseerd.

Marvin\_ biedt de oplossing. Deze dienst is deels automatisch en deels manueel en geeft je continu inzicht in de security van je infrastructuur.

### Waarom een dagelijkse scan?

Veel organisaties zoeken naast de periodieke pentests naar een manier om structureel zicht te houden op hun online omgeving en eventuele nieuwe kwetsbaarheden. Zij willen al het mogelijke doen om de veiligheid en beschikbaarheid van de infrastructuur te borgen. Wanneer de infrastructuur een cruciale asset van een organisatie is dan is de impact van kwetsbaarheden te groot om risico's te nemen.

### Vulnerability scanning in het kort

- > In één oogopslag inzicht in de meest urgente kwetsbaarheden in jouw infrastructuur.
- > Een geautomatiseerde basischeck op de security van de online assets.
- > Er wordt tijd gestoken in de kwetsbaarheden, niet in false positives.
- > Direct contact met een Computest Security Specialist zorgt voor de juiste begeleiding zodat problemen snel kunnen worden opgelost.

### Security in DevOps

Security hoort thuis in het ontwikkelproces, als onderdeel van de automation van DevOps teams. Dat zorgt voor continuïteit en zichtbaarheid in een CI/CD straat. Marvin\_ helpt het DevOpsteam continu de security van de infrastructuur bewaken, ook bij continue deployments.

### Geen false positives (meer)

Sommige organisaties maken reeds gebruik van een automatische security scantool. Zij zijn vaak veel tijd kwijt met het analyseren en filteren van de resultaten, of blijken niet over de benodigde expertise te beschikken om dit op een juiste en efficiënte manier te doen.



# Hoe gaat Marvin\_ te werk?

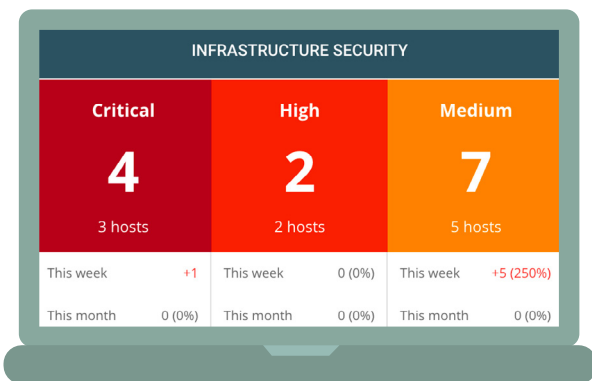


## 1. Dagelijkse security scan

Marvin\_ doet een dagelijkse security scan op de gehele infrastructuur. Hij gebruikt hiervoor bestaande en bewezen scantools.

## 2. Persoonlijk advies: analyse & validatie

De resultaten van de scan worden elke werkdag geverifieerd door een ervaren Security Specialist die bekend is met de omgeving en risico's van de klant. De specialist bepaalt welke bevindingen voor de klant relevant zijn en markeert deze als zodanig in de Marvin\_ Portal. Je kunt de chatfunctionaliteit gebruiken om met de Security Specialist te communiceren.



## 3. De Marvin\_ portal

De portal biedt in één dashboard de status van de beveiliging van de omgeving. Dit bevat onder andere:

- > het aantal relevant beoordeelde kwetsbaarheden dat in de laatste scan is gedetecteerd;
- > de hosts met de meeste kwetsbaarheden, die structurele aandacht verdienen;
- > de nieuwste en laatst aangepaste kwetsbaarheden;
- > de comments die zijn geplaatst bij de kwetsbaarheden door zo wel de klant als door een Computest Security Specialisten;
- > trendrapport: hoeveel kwetsbaarheden zijn er dagelijks bijgekomen of verdwenen.

## Marvin\_ kan veel meer!

Naast een dagelijkse security scan op de infrastructuur kan Marvin\_ desgewenst ook dagelijks inzicht geven in de performance en beschikbaarheid van jouw webapplicatie(s).

Treden responstijden buiten de grenswaarden? Ontstaan er fouten bij het openen van webpagina's, of in klikpaden en transacties?

Marvin\_ stuurt je direct een alert zodat je snel kunt ingrijpen. Onze Performance Specialisten kijken mee naar de resultaten van de monitoring en zijn beschikbaar voor analyse en overleg.

## Meest gevonden kwetsbaarheden

1. Poorten die per ongeluk open zijn
2. Software die security-patches nodig heeft
3. Gebreken in SSL/TLS configuraties

## Wat kost Marvin\_?

De exacte prijs van de hybride vulnerability scandienst is afhankelijk van de omvang en complexiteit van de te scannen omgeving. Op basis hiervan wordt een vast maandbedrag afgesproken. De dienst kan gecombineerd worden afgenomen met de hybride Application Monitoring dienst (APM), waarbij de kosten van de portal gelijk blijven.

Wil je meer weten? Of heb je interesse in een demo? Bel naar 088 - 733 13 37 of stuur een mail naar [sales@computest.nl](mailto:sales@computest.nl).

