Solvinity
Secure Managed Cloud

CYBERSECURITY ONDERZOEK

Solvinity Cybersecurity Report | **2025**

Inhoud

Introductie

Het merendeel van bedrijven met meer dan 200 medewerkers is de laatste jaren serieus met security aan de slag gegaan. Elk jaar hebben organisaties meer vertrouwen dat ze voldoende weerstand kunnen bieden tegen cyberaanvallen. Toch lijkt dit vertrouwen wat misplaatst.

Het aantal organisaties dat schade heeft opgelopen door cyber-aanvallen blijft nog steeds elk jaar stijgen. Ook internationale gebeurtenissen zoals de NAVO-top in Den Haag leiden tot een toename van cyberaanvallen.[1] Deze ontwikkelingen benadrukken hoe geopolitieke gebeurtenissen directe gevolgen kunnen hebben voor de digitale weerbaarheid van organisaties in Nederland.

In dit onderzoeksrapport analyseren we hoe weerbaar organisaties zijn, welke maatregelen zij nemen en hoe dit zich verhoudt ten opzichte van vorige jaren.

Voor dit onderzoek vroegen we in samenwerking met Panelwizard 453 IT-professionals uit Nederland naar hun ervaringen en aanpak. Deze professionals waren allen actief bij organisaties met minstens 200 medewerkers en verantwoordelijk of medebeslissend op IT-gebied. De inzichten uit het onderzoek zijn aangevuld met duiding en reflectie van Marc Guardiola (CTO bij Solvinity) en Kees Stammes (CEO bij Securify). Waar mogelijk hebben we de resultaten vergeleken met de resultaten van 2023 en 2024.

Met deze publicatie bieden we organisaties handvatten om tijdig en effectief in te spelen op de toenemende noodzaak van digitale weerbaarheid en security.

[1] https://www.ncsc.nl/actueel/nieuws/2025/06/23/opnieuw-ddos-aanvallen-rondom-navo-top-vervoerssector-ook-doelwit

Managementsamenvatting

Veel organisaties worstelen met het verkrijgen van volledig inzicht in en controle over hun eigen IT-infrastructuur. Dit gebrek aan zichtbaarheid vormt de grootste security-uitdaging en leidt ertoe dat bedrijven kwetsbaarder zijn voor beveiligingsincidenten. Vooral bij het installeren van patches en updates blijkt dat ruim een zesde van de organisaties hier soms weken tot maanden over doet, terwijl slechts een minderheid dit binnen enkele uren oppakt. Het tekort aan capaciteit op de IT-afdeling wordt hierbij het vaakst als oorzaak genoemd.

Op het gebied van geavanceerde beveiligingsmaatregelen maakt 66% van de organisaties gebruik van een Security Operations Center (SOC). Organisaties die geen SOC-functionaliteit inzetten, noemen de kosten en het beperkte budget als voornaamste redenen hiervoor. Ook bij het uitvoeren van Red Teaming-oefeningen, die bedoeld zijn om de weerbaarheid van de organisatie te testen, zijn kosten en budget vaak een drempel. Hoewel 72,4% van de organisaties met een SOC wel eens dergelijke oefeningen uitvoert, gebeurt dit bij 35,7% op regelmatige basis en voert 36,7% deze oefeningen af en toe uit.

Samenvattend blijkt dat het vergroten van zichtbaarheid, het versnellen van patch- en updateprocessen en het vergroten van de capaciteit op de IT-afdeling essentieel zijn om de digitale weerbaarheid te verhogen. Verder zijn investeringen in SOC-functionaliteit en de structurele inzet van Red Teaming en Continuous Security Testing van groot belang, maar vormen kosten en budget hierbij een aanhoudende uitdaging. Organisaties die hier desondanks toch in slagen, zijn aantoonbaar beter voorbereid op het groeiende dreigingslandschap.

Belangrijkste bevindingen

Inzicht

- De grootste security uitdagingen voor bedrijven kunnen worden samengevat als het ontbreken van volledig inzicht en het niet 'in control' zijn van de eigen infrastructuur.

Tijdsduur, uitstel en afstel patches en updates

- Bij ruim 45,5% van de organisaties duurt het installeren van patches en updates enkele dagen, weken tot zelfs maanden. Van alle organisaties voert 21,5% patches en updates binnen enkele uren uit. Voor 20,8% verschilt het per keer. De rest van de respondenten geeft aan (sommige) systemen helemaal niet meer te patchen of het helemaal niet te weten.
- Onvoldoende capaciteit op de IT-afdeling wordt het vaakst genoemd als oorzaak van het uit- of afstellen van patching en updating (24,5%).

Security Operations Center

- Tweederde van de ondervraagde organisaties maakt gebruikt van een SOC.
- Bij organisaties die geen gebruik maken van een SOC worden kosten en het beschikbare budget als belangrijkste redenen genoemd.

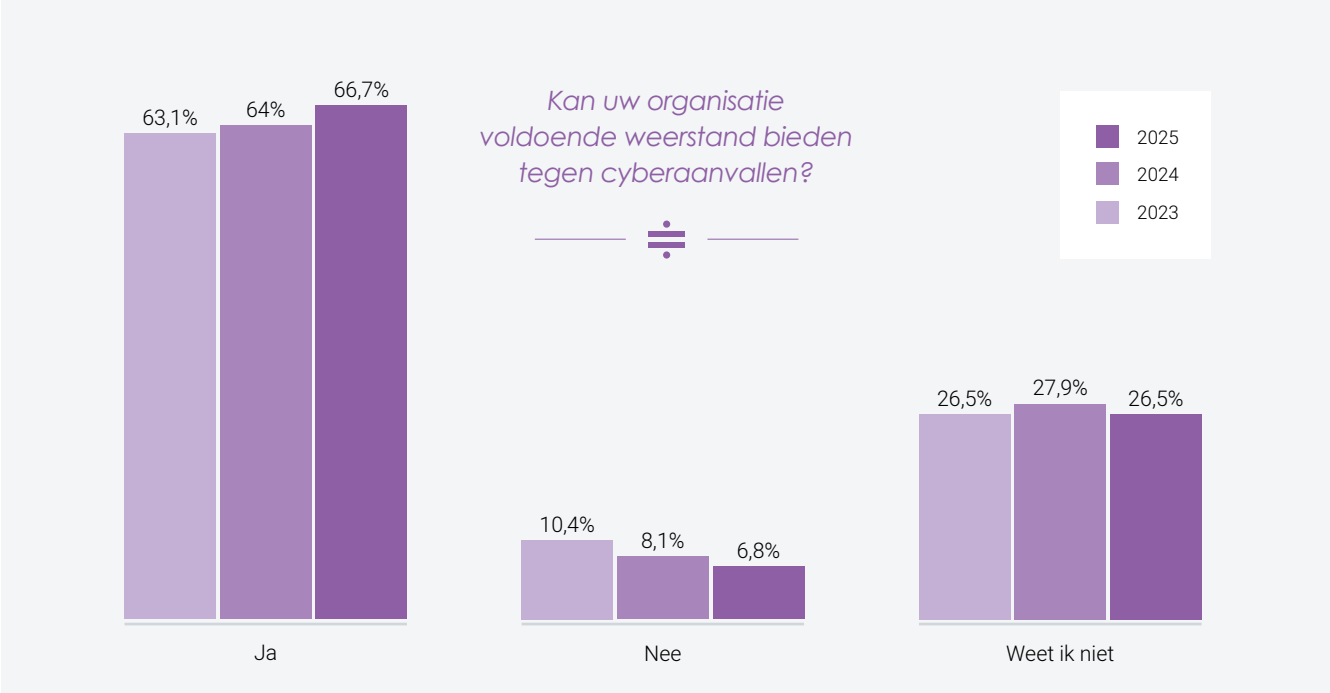
Red teaming

- Ruim 72% van de organisaties met een SOC voert wel eens Red-Teaming oefeningen uit, 35,7% doet dit regelmatig.
- De grootste uitdaging bij het integreren en overstappen naar Continuous Security Testing zijn kosten en budget (40,1%).

Hoe goed zijn organisaties gewapend tegen cyberaanvallen?

Organisaties geven aan steeds beter te zijn bewapend tegen cyberaanvallen. In 2025 geeft 66,7% van de organisaties aan voldoende weerstand te kunnen bieden tegen cyberaanvallen, ten opzichte van 64% in 2024 en 63,1% in 2023. Dit lijkt een positieve trend, maar het betekent dat een derde van de organisaties zich nog steeds niet goed kan wapenen.

"Een derde van de organisaties kan zich nog steeds niet goed wapenen tegen cyberaanvallen."

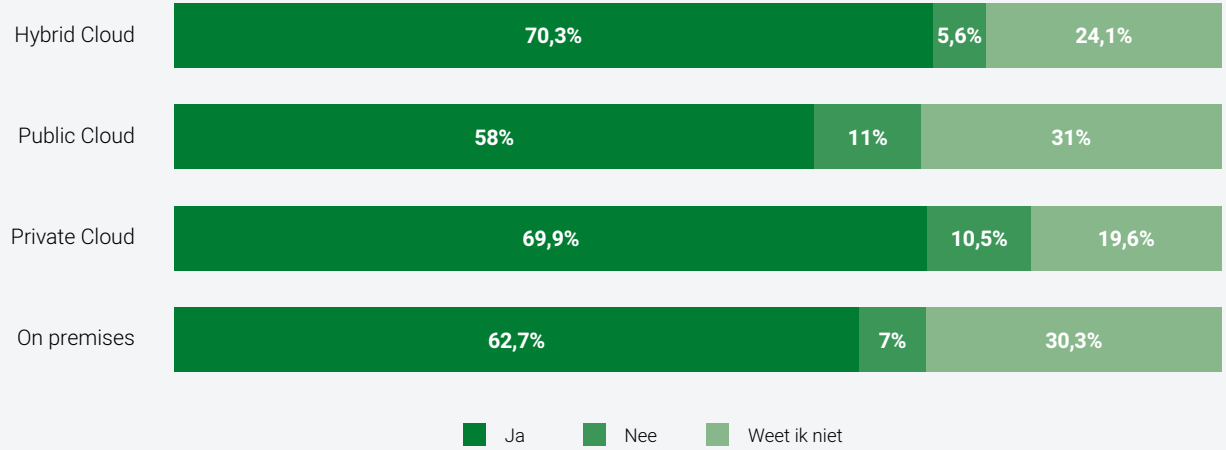


Organisaties van tussen de 500-999 medewerkers lijken het meest zeker in het bieden van weerstand (71,7%). Kleinere organisaties van tussen de 200-499 medewerkers lijken minder zeker van hun zaak. Hier verwacht 59% weerstand te kunnen bieden tegen cyberaanvallen.

Kan uw organisatie voldoende weerstand bieden tegen cyberaanvallen?

Net zoals vorig jaar, lijkt het vertrouwen bij IT-professionals die de public cloud gebruiken het laagst (58,1%).

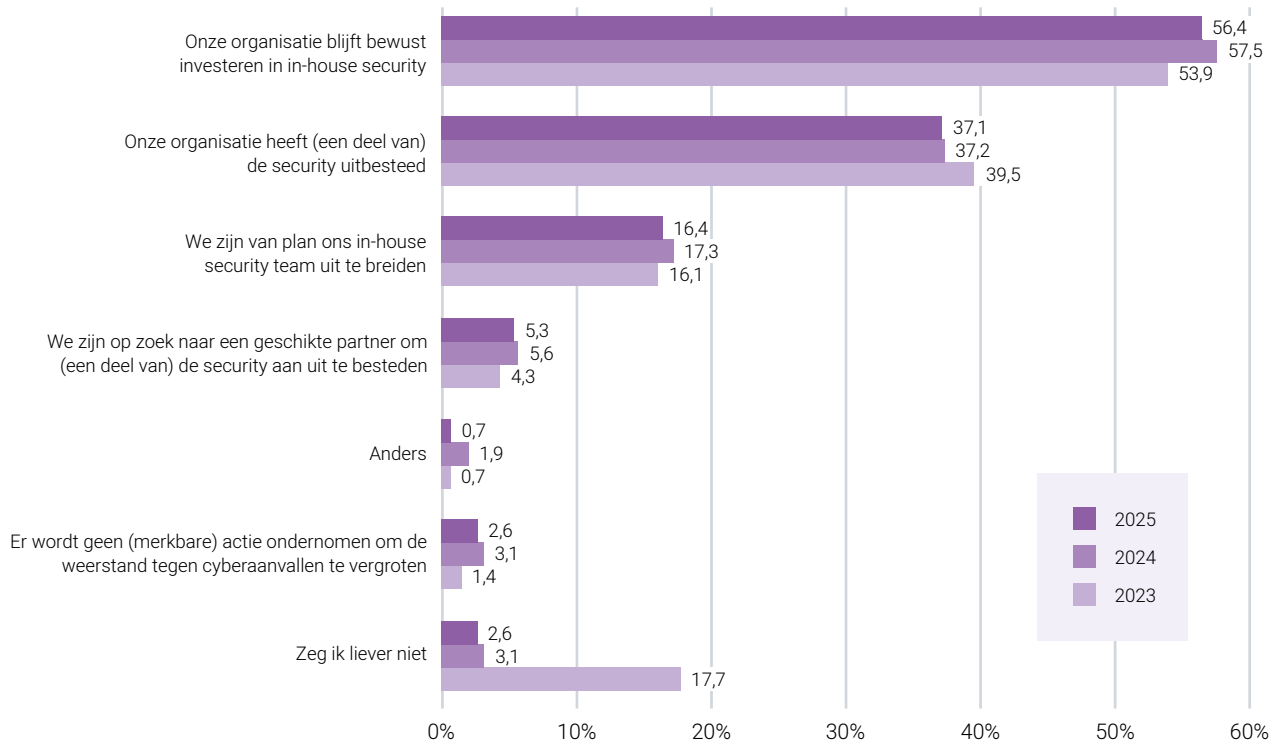
Kan uw organisatie voldoende weerstand bieden tegen cyberaanvallen?



Wat doen organisaties om cyberaanvallen tegen te gaan?

Om cyberaanvallen te voorkomen, kiest het grootste deel van de organisaties ervoor om bewust te blijven investeren in eigen securitycapaciteit: 56,4% geeft aan hun security voornamelijk in-house te organiseren. Daarnaast besteedt 37,1% de beveiliging geheel of gedeeltelijk uit aan externe partijen.

Op welke manieren wapent uw organisatie zich tegen cyberaanvallen? U kunt meerdere antwoorden geven.



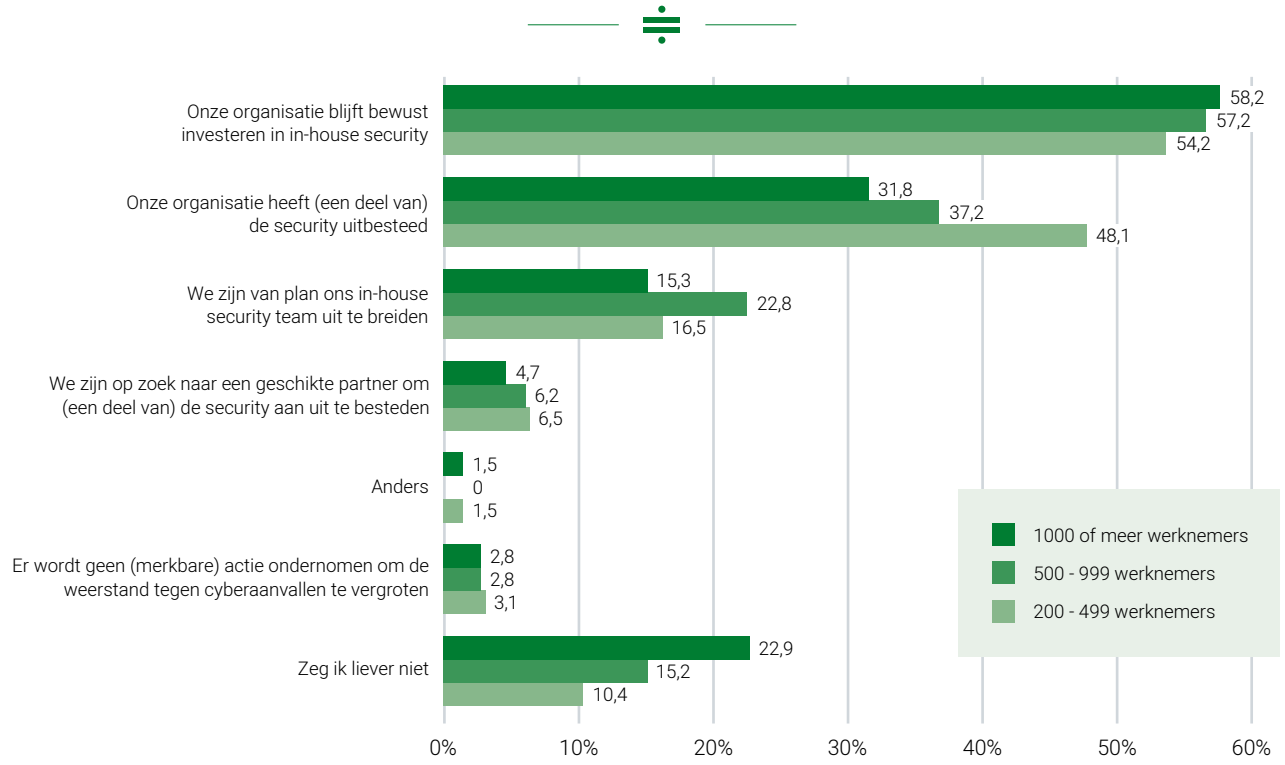
Opvallend

Meer dan 50% van de organisaties, ongeacht het aantal werknemers, investeert bewust in in-house security en houdt zo de beveiliging (deels) in eigen hand.

Opvallend is dat vooral organisaties met 200-499 medewerkers vaker kiezen voor uitbesteding van (een deel van) hun security. Dit komt in de meeste gevallen doordat zij minder interne capaciteit hebben om alle benodigde expertise en technologie zelf op peil te houden.

De keuze tussen in-house security en uitbesteding (of een combinatie van beiden) hangt sterk af van de omvang en mogelijkheden van een organisatie. Voor veel kleinere organisaties biedt uitbesteding een praktische oplossing om toch toegang te krijgen tot specialistische kennis en continue monitoring. Grote organisaties kiezen vaker voor het opbouwen van een intern securityteam, maar blijven ook alert op situaties waarin aanvullende externe ondersteuning nodig is. Het belangrijkste blijft dat organisaties, ongeacht de gekozen vorm, blijven investeren in effectieve beveiligingsmaatregelen om zich te wapenen tegen het groeiende aantal cyberdreigingen.

Op welke manieren wapent uw organisatie zich tegen cyberaanvallen? U kunt meerdere antwoorden geven.

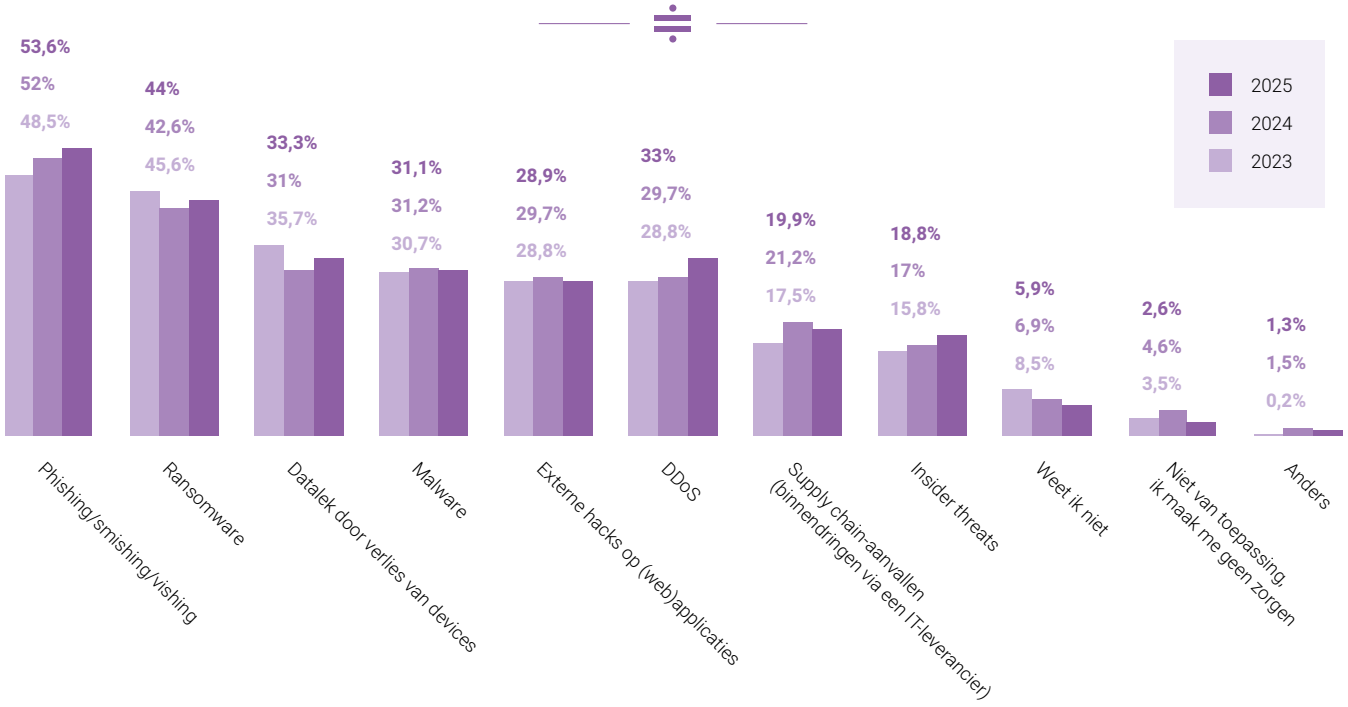


Grootste cyberdreigingen

In 2025 zien organisaties cyberdreigingen als phishing/smishing/vishing (53,6%), ransomware (44%) en een datalek door het verlies van devices (32,1%) als grootste zorgen. Deze resultaten laten zien dat organisaties zich steeds beter bewust zijn van de breedte van het dreigingslandschap, van gerichte aanvalsvormen zoals phishing tot meer traditionele risico's als dataverlies door verloren apparaten.

Het blijft voor organisaties essentieel om een combinatie van technische maatregelen (zoals endpoint security en back-ups) en bewustwordingsprogramma's in te zetten om de impact van deze dreigingen te minimaliseren en medewerkers weerbaar te maken tegen de meest voorkomende aanvalsmethoden.

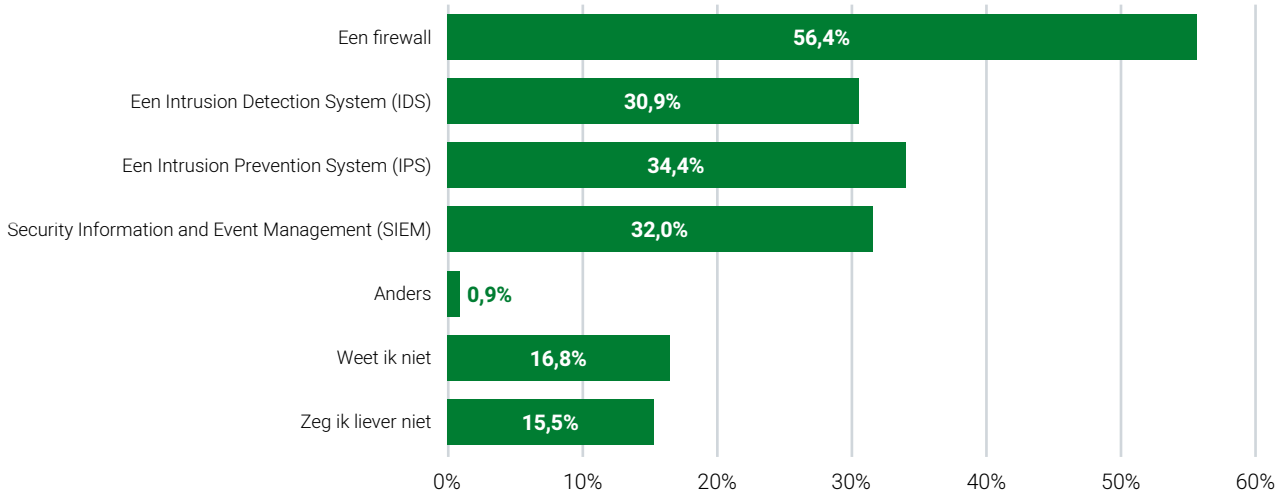
Over welke cyberdreigingen maakt u zich het meest zorgen?
U kunt meerdere antwoorden geven.



Monitoren van verdacht netwerkverkeer

Veruit de meest ingezette maatregel om verdacht netwerkverkeer te monitoren en te weren is een firewall; ruim de helft (56,4%) geeft dit antwoord. Organisaties zetten daarnaast (ook) een Intrusion Prevention System (IPS) (34,4%), een Security Information en Event Management (SIEM) (32%) en/of een Intrusion Detection System (IDS) (30,9%) in. Hoewel de firewall nog steeds de basis vormt van netwerkbeveiliging, zien we dat steeds meer organisaties kiezen voor een gelaagde aanpak door meerdere beveiligingssystemen te combineren. Dit wijst op een groeiend besef dat alleen een firewall niet langer volstaat tegen steeds geavanceerdere bedreigingen. Het inzetten van extra detectie- en analysetools zoals IDS, IPS en SIEM helpt organisaties om sneller in te spelen op verdachte activiteiten en incidenten effectiever te herkennen en te onderzoeken. Investeren in een combinatie van deze systemen verhoogt de kans om aanvallen tijdig te detecteren en te mitigeren.

Welk van onderstaande maatregelen zet uw organisatie in om verdacht netwerkverkeer te monitoren en te weren? U kunt meerdere antwoorden geven.



"Het is cruciaal dat organisaties beginnen met een grondige inventarisatie van hun infrastructuur en netwerken, aangevuld met een gedegen risicoanalyse."

Grootste security-uitdaging

Het gedegen implementeren van de juiste beveiligingsmaatregelen (27,1%), het gericht identificeren van te beschermen processen, systemen en data (22,4%) en het tijdig detecteren van security incidenten (18,4%) worden als grootste security-uitdagingen gezien. Deze top drie kan worden samengevat als het ontbreken van volledig inzicht in de eigen infrastructuur, met als resultaat dat een organisatie weinig tot geen controle heeft.

Het is cruciaal dat organisaties beginnen met een grondige inventarisatie van hun infrastructuur en netwerken, aangevuld met een gedegen risicoanalyse. Dit biedt het noodzakelijke overzicht om goed te bepalen welke systemen en data beschermd moeten worden. Op basis van deze inzichten kunnen organisaties gerichte beveiligingsmaatregelen kiezen én beter inspelen op actuele dreigingen. Door te investeren in inzicht en monitoring wordt niet alleen de weerbaarheid vergroot, maar ontstaat ook de basis voor een continu verbeterende securitystrategie.

Wat is de grootste security-uitdaging binnen uw IT-omgeving?

Security Testing: een vals gevoel van veiligheid

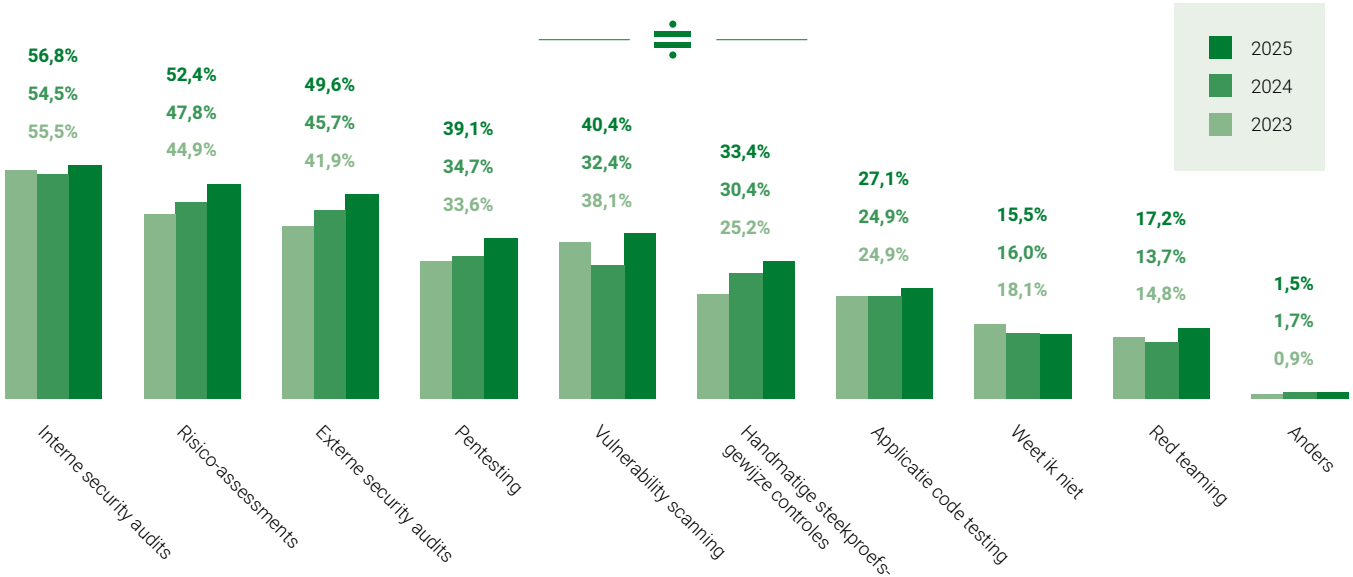
Elk jaar vragen wij organisaties welke testmethoden zij inzetten om hun security te toetsen. Net als in 2023 en 2024 zijn ook in 2025 interne security audits de meest gebruikte methode (56,8%). Ook risico assessments (52,4%) en externe security audits (49,6%) worden nog steeds door veel bedrijven als testmethode ingezet.

Interne audits zijn volgens Kees Stammes, CEO bij Securify, slechts een papieren werkelijkheid. De echte werkelijkheid wordt getest door het uitvoeren van pentesten en Red Teaming opdrachten.

Daarmee ga je een stap verder en simuleer je echte aanvallen om de cyberweerbaarheid te testen.

Dit wordt door 17,2% van alle respondenten aangegeven als gebruikte methode. “Ik durf te stellen dat deze 17,2% echt weerbaar is tegen cyberaanvallen. De rest die niet aan Red Teaming doet, doet aan schijnveiligheid. Het gegeven dat 42% van de respondenten in de volgende paragraaf aangeeft dat de topprioriteit meer benodigde kennis is, versterkt dit gevoel”, aldus Kees.

Welke methoden gebruikt uw organisatie om de security te toetsen?
U kunt meerdere antwoorden geven.



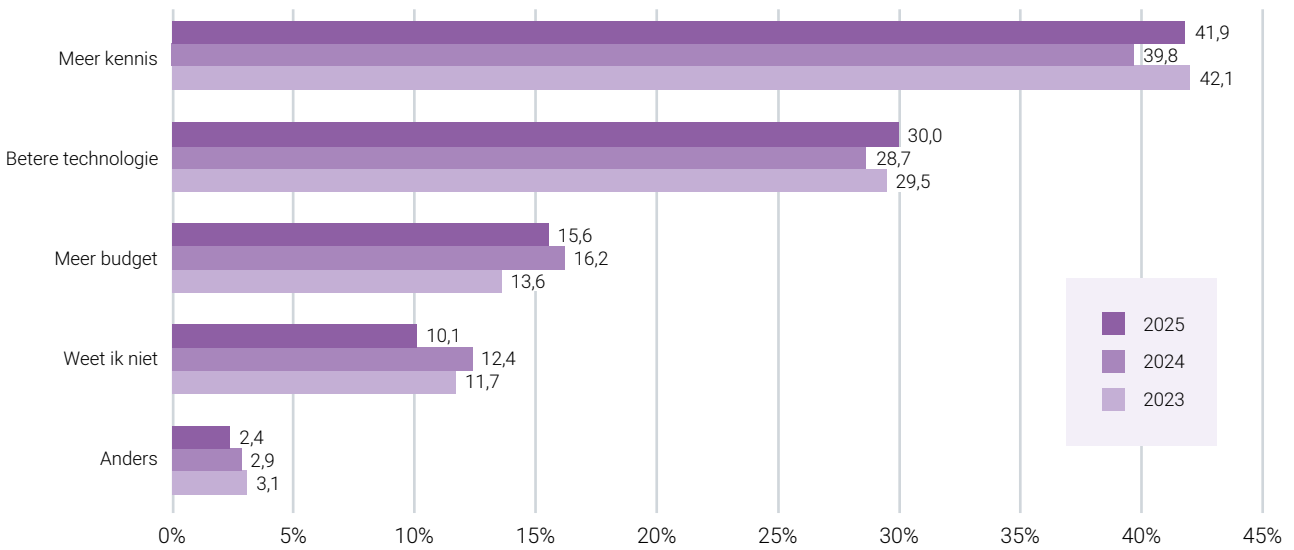
Kennis als sleutelfactor

Ook in 2025 is het vergaren van kennis nog steeds de belangrijkste prioriteit voor organisaties om zich voor te bereiden op toekomstige securityontwikkelingen (41,9%). Ook betere technologie wordt door bijna een derde van de respondenten genoemd. Budget wordt niet gezien als bottleneck, zelfs niet binnen kleinere organisaties.

De resultaten onderstrepen dat investeren in kennis cruciaal blijft om effectief in te spelen op het veranderende dreigingslandschap. Tegelijkertijd wordt duidelijk dat technologische innovatie alleen effectief is als deze samengaat met voldoende kennis binnen de organisatie. Organisaties doen er daarom goed aan te blijven investeren in de expertise van hun medewerkers, om daarmee het maximale uit hun securitymaatregelen te halen.

Consistent
Nog steeds ziet vier op de tien organisaties kennis als dé sleutel om futureproof te blijven in cybersecurity.

Wat is in uw ogen de topprioriteit om uw organisatie voor te bereiden op het gebied van toekomstige security-ontwikkelingen?

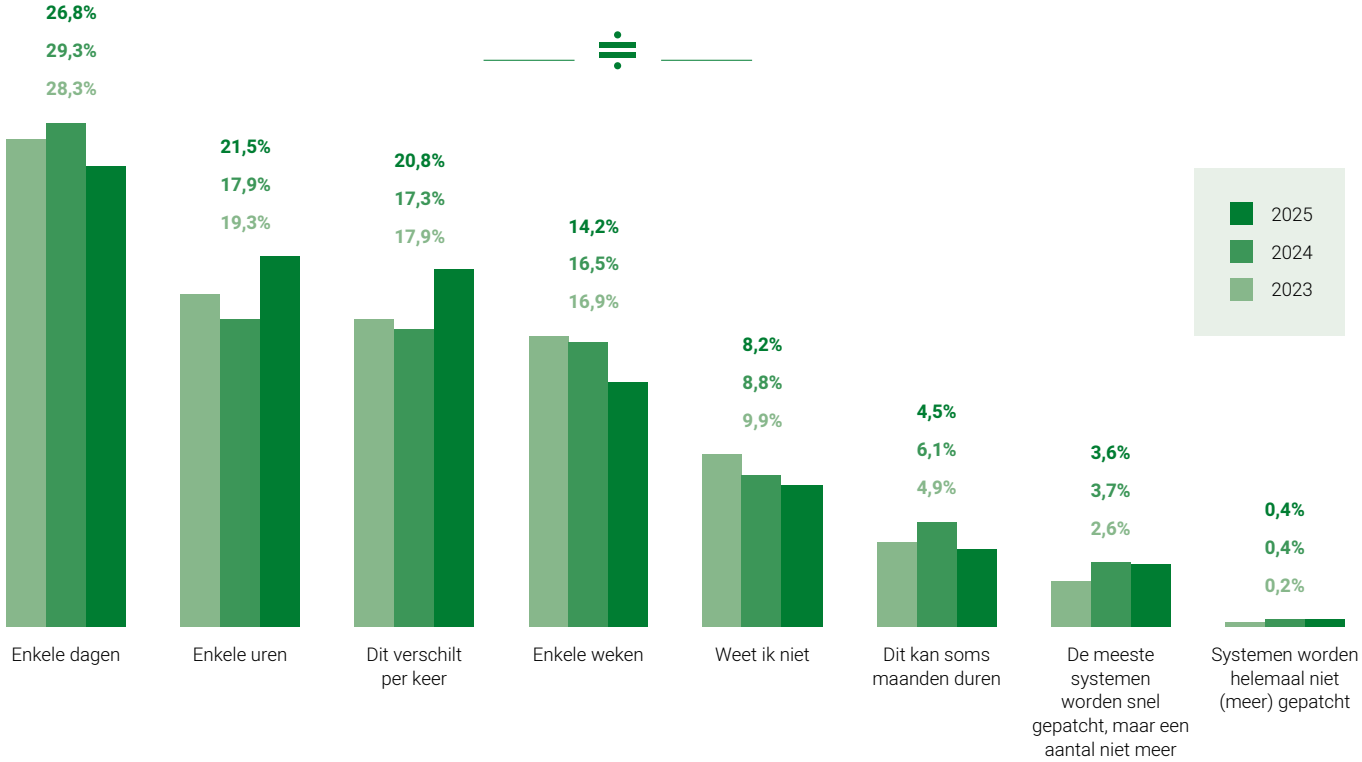


De basis nog steeds niet in orde?

Uit eerdere onderzoeken bleek al dat de basismaatregelen voor security, zoals patch management, bij veel organisaties niet op orde zijn. We zien in 2025 dat patch management nog steeds een uitdaging vormt. Veel organisaties zijn te traag met het uitvoeren van patches en updates: slechts 21,5% slaagt erin om deze binnen enkele uren te installeren. Dit vergroot het risico dat bekende kwetsbaarheden kunnen worden misbruikt.

Waar in 2024 nog 30,7% aangaf patches uit te stellen vanwege capaciteitsgebrek, is dit in 2025 gedaald naar 24,5%. Ook de vrees van management voor bedrijfscontinuïteit blijft een reden voor het af- of uitstellen van patches. In 2025 (20,1%) lijkt het percentage hoger te liggen dan in 2024 (18,6%).

Hoe lang duurt het gemiddeld voordat updates en patches worden geïnstalleerd bij uw organisatie?



Waarom wordt (soms) besloten patching of updating uit/af te stellen?
U kunt meerdere antwoorden geven.

Volgens Marc Guardiola is het uitstellen van patches een schrikbarend fenomeen. “Het is alom bekend dat hackers in staat zijn om hier binnen enkele uren (en soms nog sneller) misbruik van te maken. Een aanbeveling is dan ook om een vulnerability- en patch managementproces te ontwikkelen dat zoveel mogelijk is geautomatiseerd is en regelmatig geëvalueerd wordt.”

3 tips om je patch management op orde te krijgen

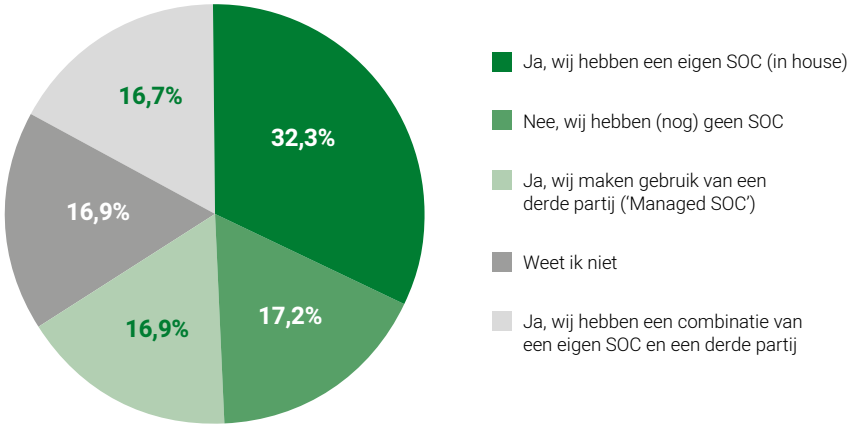
- Vergroot het kennisbewustzijn bij het management zodat kwetsbaarheden de juiste prioriteit krijgen
- Automatiseer patch- en vulnerability management om sneller en efficiënter te kunnen reageren
- Stel één eindverantwoordelijke aan die structureel monitort en rapporteert om meer controle en overzicht te krijgen

Het belang van een SOC

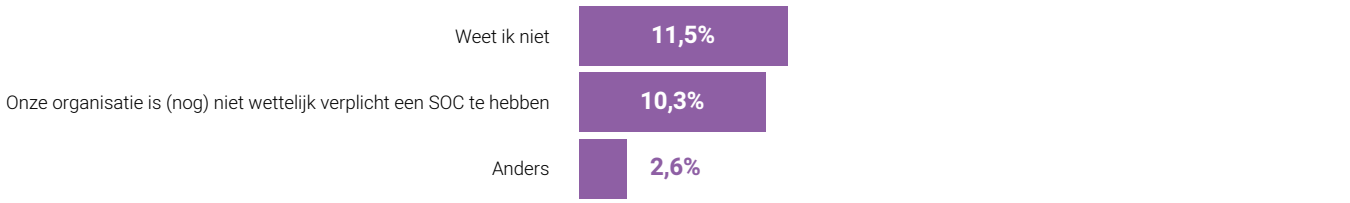
Opvallend
Kosten en budget zijn voor 42,3% de grootste drempel om een SOC in te richten.

Uit het onderzoek blijkt dat 65,9% van de organisaties gebruikmaakt van een Security Operations Center (SOC). Van alle organisaties geeft 17,2% aan nog altijd geen SOC te hebben. Zij beschikken dus niet over adequate detectie- en responsecapaciteit om snel op security-incidenten te reageren.

Maakt uw organisatie gebruik van een Security Operations Center met een 24/7 detectie en response capaciteit?



Waarom heeft uw organisatie (nog) geen SOC?
U kunt meerdere antwoorden geven.



Deze vraag is in 2025 aan **78 personen** van verschillende organisaties, die nog **geen SOC** hebben, gesteld.

Bij deze vraag zijn meerdere antwoorden mogelijk, waardoor de percentages sommeren tot meer dan 100%.

De belangrijkste drempel blijkt voor veel organisaties het kostenplaatje: 42,3% noemt de kosten en het beschikbare budget als grootste belemmering.

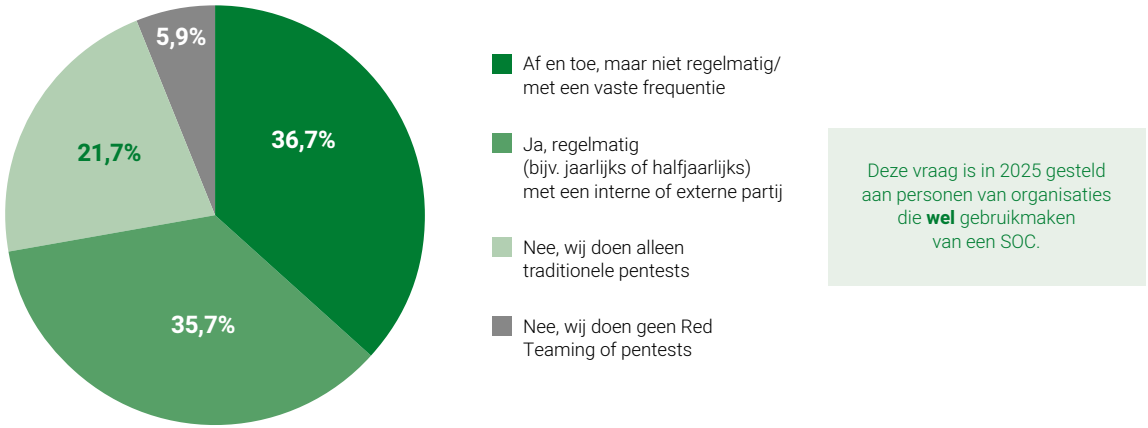
Hoewel kosten vaak als struikelblok worden genoemd, blijkt volgens in de praktijk dat de investeringen voor een Managed SOC doorgaans lager uitvallen dan veel organisaties verwachten. Daarom is het belangrijk om de mogelijkheden van een Managed-SOC in kaart te brengen met een haalbaarheidsonderzoek.

Effectiviteit van een SOC meten

Zorgwekkend
Eén op de vijf organisaties (21,7%) vertrouwt nog altijd uitsluitend op traditionele pentests.

Van de organisaties die gebruik maken van een SOC, geeft 72,4% aan de effectiviteit hiervan te toetsen met Red Teaming-oefeningen. Toch zien we dat ruim één op de vijf (21,7%) nog altijd uitsluitend vertrouwt op traditionele pentests. Dit is zorgelijk, want aanvallers opereren niet volgens een vast schema en beperken zich niet tot jaarlijkse aanvallen met een beperkte scope.

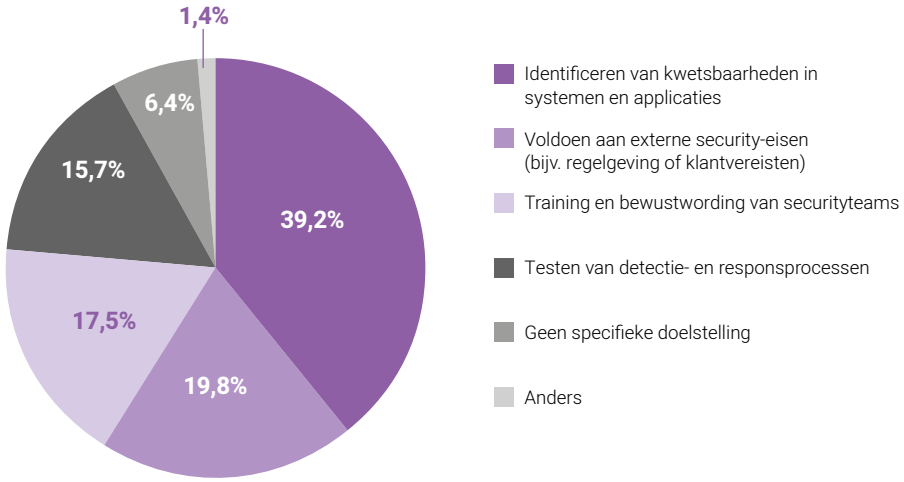
Voert uw organisatie regelmatig Red Teaming-oefeningen uit om de effectiviteit van uw SOC te testen?



Deze vraag is in 2025 gesteld aan personen van organisaties die **wel** gebruikmaken van een SOC.

Red Teaming wordt door organisaties vooral ingezet om kwetsbaarheden te identificeren (39,2%) en om te voldoen aan externe security-eisen (19,8%). Dit laat zien dat Red Teaming niet alleen waardevol is voor de eigen veiligheid, maar ook steeds belangrijker wordt voor compliance en het aantonen van security-inspanningen richting toezichthouders en partners.

Wat is het primaire doel van Red Teaming binnen uw organisatie?



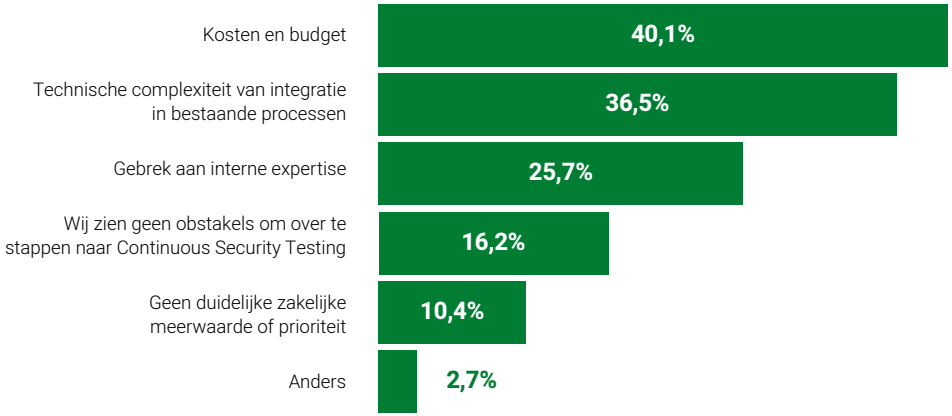
Deze vraag is in 2025 gesteld aan personen van organisaties die **wel** gebruikmaken van een SOC.

Van jaarlijks pentesten naar Continuous Security Testing

Hoewel het merendeel van de organisaties vooruitgang boekt met geavanceerde testmethoden als Red Teaming, blijft er op het gebied van pentesten ruimte voor verbetering. Door vaker te kiezen voor continue testmethodes zoals Continuous Security Testing, krijgen organisaties een beter en actueler beeld van hun daadwerkelijke weerbaarheid. Op deze manier wordt security een vast onderdeel van het proces, waarmee nieuwe releases direct gemonitord kunnen worden. Helaas ziet ruim 40% van de organisaties kosten en budget als grootste uitdaging bij het overstappen naar Continuous Security Testing. Dit terwijl het kosten/batenplaatje vaak juist positief uitvalt: het voorkomt dure hersteltrajecten achteraf, verkort de doorlooptijd bij audits, vermindert impactvolle incidenten en zorgt ervoor dat ontwikkelaars veiligere code gaan schrijven. Volgens Kees Stammes (CEO Securify) zou dit daarom geen uitdaging moeten zijn:
"Security is geen kostenpost, maar een investering die zich dagelijks terugbetaalt in bedrijfscontinuïteit, klantvertrouwen en concurrentievoordeel. Juist met Continuous Security Testing bespaar je op de lange termijn meer dan je uitgeeft."

Positieve uitzondering
Eén op de zes organisaties ziet géén obstakels om over te stappen naar Continuous Security Testing.

Wat zijn voor uw organisatie de belangrijkste obstakels om over te stappen naar Continuous Security Testing?



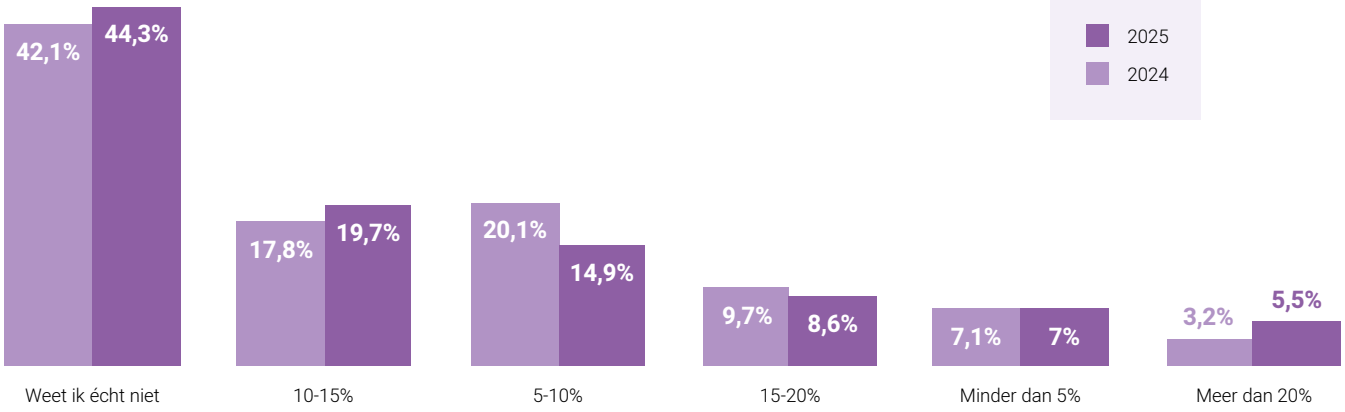
Deze vraag is in 2025 aan **222 personen** van verschillende organisaties, die **Continuous Security Testing** hebben geïmplementeerd of overwegen in CI/CD.

Bij deze vraag zijn meerdere antwoorden mogelijk, waardoor de percentages sommeren tot meer dan 100%.

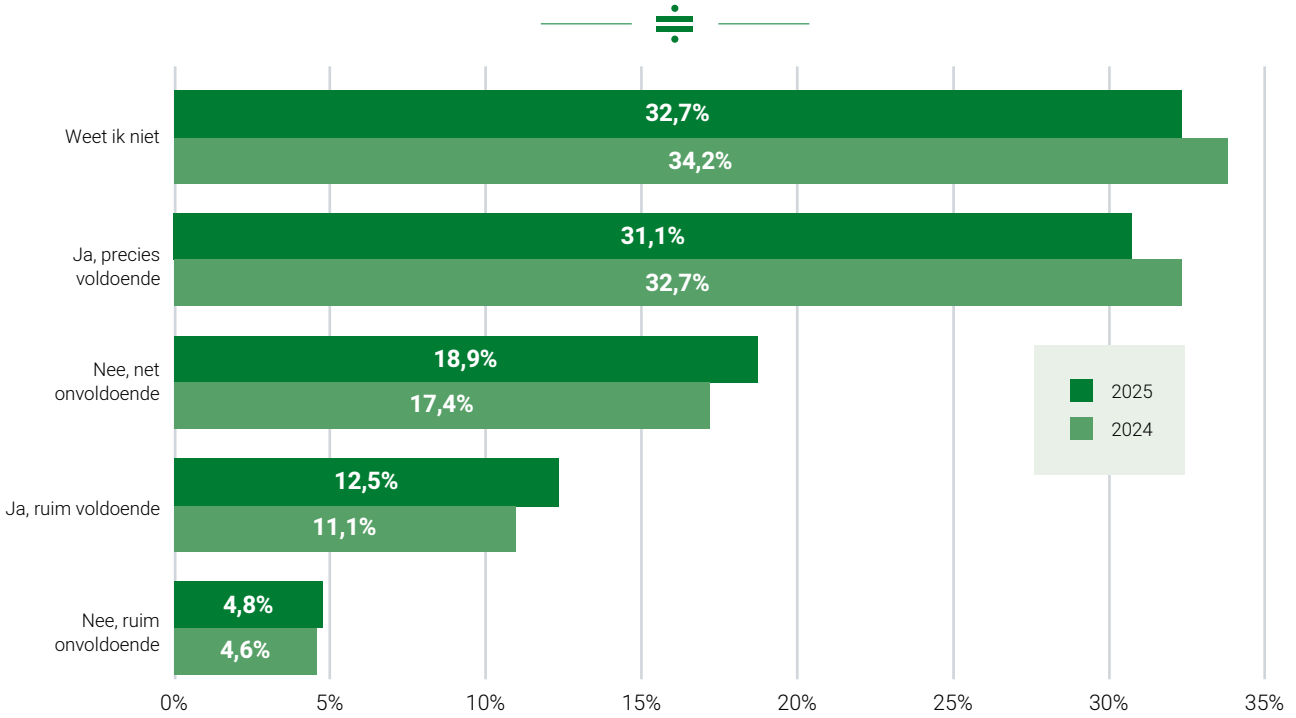
Het IT-securitybudget

Uit het onderzoek blijkt dat 19,7% van de respondenten aangeeft zo'n 10-15% van het totale IT-budget te besteden aan IT-security. Bijna 15% van de organisaties investeert 5-10% van hun IT-budget in security, terwijl het aandeel organisaties dat minder dan 5% uitgeeft nagenoeg gelijk blijft aan vorig jaar.

Hoeveel procent van het IT-budget van uw organisatie gaat naar IT-security?

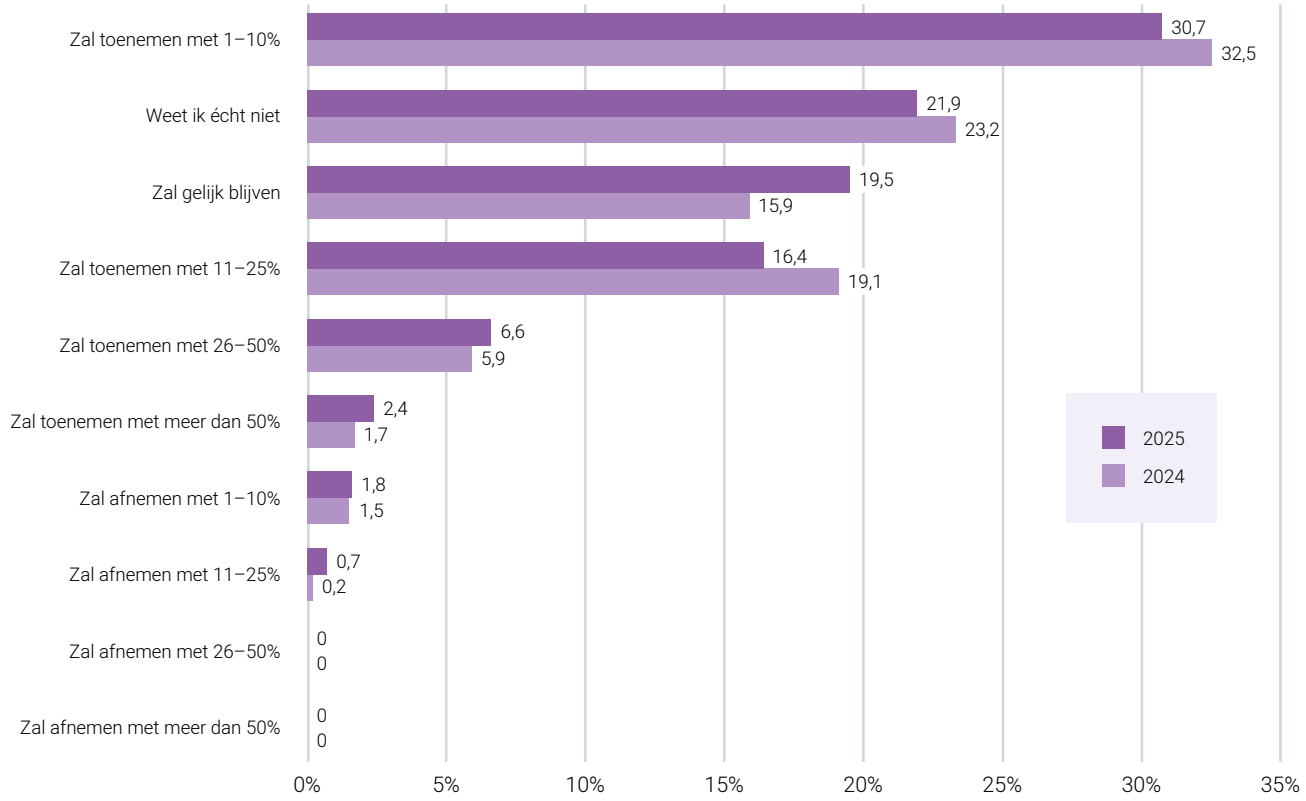


Is het huidige budget voor security voldoende om de security van uw organisatie te waarborgen?



Wat betreft het gevoel over de huidige budgetten vindt 31,1% van de respondenten het beschikbare securitybudget precies voldoende. Daarnaast geeft 12,5% zelfs aan dat het budget ruim voldoende is.

Verwacht u dat het budget dat uw organisatie in 2025 zal besteden aan IT-security zal toenemen of afnemen ten opzichte van 2024? Ook als u het niet precies weet, vragen wij u om een schatting te maken.



Opvallend is dat het vertrouwen in verdere groei groot is: meer dan de helft (56,1%) verwacht dat het budget voor IT-security in 2025 zal toenemen. Bijna 20% denkt dat het budget gelijk blijft, terwijl slechts 2,5% een daling voorziet.

Hoewel veel organisaties redelijk tevreden zijn over het huidige IT-securitybudget, blijft het zaak om alert te blijven op ontwikkelingen en te blijven investeren. De groeiende dreigingen en toename in complexiteit van cyberaanvallen vragen om voortdurende aandacht en voldoende middelen. Door structureel te investeren in IT-security en tijdig het budget bij te stellen waar nodig, kunnen organisaties blijvend inspelen op nieuwe risico's en hun digitale weerbaarheid vergroten.

Continu testen loont
Maak continu testen de norm: zo verschuift security van momentopname naar een permanent concurrentievoordeel.

Aanbevelingen voor een toekomstbestendige securitystrategie

Om digitale dreigingen het hoofd te bieden, is meer nodig dan losse maatregelen. Een effectieve securitystrategie vraagt om samenhang, helder inzicht en continue verbetering. Onderstaande aanbevelingen helpen organisaties om hun weerbaarheid te vergroten en hun beveiliging klaar te maken voor toekomstige uitdagingen.

1 Investeer in inzicht en monitoring

Een goed overzicht van infrastructuur en netwerken, ondersteund door een risicoanalyse, helpt organisaties om gericht te bepalen welke systemen en data beveiligd moeten worden. Dit inzicht maakt het mogelijk om passende beveiligingsmaatregelen te nemen en snel in te spelen op dreigingen, waardoor de weerbaarheid en securitystrategie continu verbeteren.

2 Zorg dat de basismaatregelen in orde zijn

Basismaatregelen zoals patch management schieten vaak tekort, ondanks groeiende dreigingen. Het is daarom belangrijk het kennisniveau bij management te verhogen, patch- en vulnerability management te automatiseren en één eindverantwoordelijke aan te stellen. Door hierin te investeren, wordt de securitybasis versterkt en het risico op incidenten aanzienlijk verminderd.

3 Doe een haalbaarheidsonderzoek naar een Managed SOC

Hoewel kosten vaak als struikelblok gelden, kan de investering in een Managed SOC lager uitvallen dan verwacht. Een haalbaarheidsonderzoek helpt om objectief te bepalen of deze oplossing past bij de organisatie en betaalbaar is, terwijl het de detectie- en responsecapaciteit én weerbaarheid tegen incidenten versterkt.

4 Maak continu testen de norm binnen de organisatie

Maak continu testen de norm. De groeiende dreigingen en toename in complexiteit van cyberaanvallen vragen om voortdurende aandacht en voldoende middelen. Daarom zijn jaarlijkse pentesten simpelweg niet meer voldoende. Met Continuous Security Testing wordt security een geïntegreerd, doorlopend proces dat meebeweegt met de snelheid van ontwikkeling. Je hebt altijd realtime inzicht in kwetsbaarheden, kunt direct ingrijpen bij nieuwe risico's en aantonen dat security dagelijks goed is geborgd in het ontwikkel- en beheerproces. Zo verschuift security van een momentopname naar een permanent concurrentievoordeel en ben je elke dag aantoonbaar in control.

Oplossingen voor een beheersbare en weerbare organisatie

Solvinity ondersteunt organisaties bij het versterken van hun digitale weerbaarheid. De inzichten uit dit onderzoek geven een beeld van de mate waarin Nederlandse bedrijven zijn voorbereid op cyberdreigingen.

Heeft jouw organisatie vragen over de eigen positie binnen dit landschap, of behoefte aan een onafhankelijke evaluatie van securitymaatregelen? Solvinity biedt ondersteuning, zowel bij het optimaliseren van bestaande IT-teams als bij het ontwikkelen en beheren van cloudplatformen met een hoge mate van beveiliging. Met diepgaande expertise, ervaring en een uitgebreid serviceportfolio helpen wij organisaties om hun IT-omgeving optimaal te laten functioneren en de security van cloudplatformen structureel te waarborgen.

Samen met onze dochteronderneming Securify bieden wij een unieke combinatie van manageability, compliance en praktisch toepasbare security. Dankzij Securify's geavanceerde tooling en ethical hacking-expertise kunnen bedrijven kwetsbaarheden in real time opsporen, testen en verhelpen, terwijl ontwikkelteams direct bruikbare feedback ontvangen. Zo tillen we beveiliging naar een continu, geïntegreerd proces dat innovatie versnelt en risico's structureel verkleint.

÷ Solvinity. Securify

WIL JE MEER WETEN?

Neem contact met ons op via
info@solvinity.com
of **+31 (0)20 36 43 600**
of bezoek onze website
https://solvinity.com/nl

Solvinity
Secure Managed Cloud

Solvinity B.V.
Postbus 23673
1100 ED Amsterdam

T +31(0)20 364 3600
E info@solvinity.com
https://solvinity.com/nl

Met secure managed cloud services ondersteunt en adviseert Solvinity organisaties met hoge beveiligingseisen in hun digitale transformatie.

	Public Cloud Private Cloud Security Services Workspace
	Solvinity onderscheidt zich op het gebied van cybersecurity met een uitgebreid portfolio aan securitydiensten en oplossingen en biedt, met een meerderheidsbelang in Securify, aanvullende diensten op het gebied van pentesting, red teaming en agile security.
	Certificeringen volgens (inter)nationale normen als ISO 27001, ISO 14001, ISO 9001, ISAE3402 Type I en II en PCI DSS. Als eerste Managed Service Provider in Nederland SOC 1 & 2 compliancerapporten voor de gehele beheeromgeving van niet alleen de private, maar ook de Azure-cloud.
	Solvinity levert aan de (rijks-)overheid, gemeenten en toonaangevende organisaties in de financiële en zakelijke dienstverlening, zoals het ministerie van Justitie en Veiligheid, Politie Nederland, Translink (OV-chipkaart), ING en Klaverblad.

300+ medewerkers	Amsterdam, Assen Amersfoort, Den Bosch		