CISCO
SECURE

Security Outcomes Study

Deel 2

De top vijf security praktijken optimaliseren

Inhoud

(Hernieuwde) kennismaking met de grote vijf 3

Belangrijkste bevindingen 4

Strategieën voor proactieve vernieuwing van technologie 6

Goed geïntegreerde security technologieën realiseren 13

Mogelijkheden voor bedreigingsdetectie en respons op incidenten ontwikkelen 19

Snel noodherstel en veerkracht garanderen 29

Conclusie en aanbevelingen 34

Over Cisco Secure 36

Bijlage: Demografische gegevens van steekproef 37

(Hernieuwde) kennismaking met de grote vijf

Het doel van de Cisco Security Outcomes Study 2021 was om te meten wat het belangrijkste is bij cyber security management. Daartoe hebben we 25 algemene security praktijken onderzocht en getest hoe deze correleren met 11 behaalde resultaten op programmaniveau. U kunt deze correlaties bekijken via een interactieve visualisatie op de website van de Cisco Security Outcomes Study 2021, waar u ook het volledige rapport kunt downloaden.

Uit de test bleek dat 5 van de 25 praktijken zich onderscheiden van de rest waar het de totale bijdrage aan het succes van security programma's in alle gemeten resultaten betreft.

In dit document richten we ons specifiek op die 'grote vijf' die het succes van security programma's bepalen om strategieën te identificeren die de effectiviteit ervan maximaliseren. De 'grote vijf' zijn:

Proactieve vernieuwing van technologie	De organisatie hanteert een strategie van proactieve vernieuwing van technologie om up-to-date te blijven met de beste IT- en security technologieën.
Goed geïntegreerde technologie	Security technologieën zijn goed geïntegreerd en werken effectief samen.
Tijdige respons op incidenten	Mogelijkheden voor respons op incidenten maken tijdig en effectief onderzoek en herstel van security gebeurtenissen mogelijk.
Nauwkeurige bedreigingsdetectie	Bedreigingsdetectiemogelijkheden bieden accuraat bewustzijn van mogelijke security gebeurtenissen zonder aanzienlijke blinde vlekken.
Snel noodherstel	Herstelmogelijkheden minimaliseren impact en verzekeren resiliency van bedrijfsfuncties die zijn getroffen door security incidenten.

De brede effectiviteit van deze praktijken roept de vraag 'Waarom?' op. Waarom zijn ze essentieel voor het behalen van succes? Door welke factoren worden ze meer of minder effectief? Hoe moeten bedrijven deze praktijken implementeren voor maximale resultaten? In dit deel van de Security Outcomes Study gaan we in op dit soort vragen.

In dit document richten we ons specifiek op die 'grote vijf' die het succes van security programma's bepalen om strategieën te identificeren die de effectiviteit ervan maximaliseren. Dat doen we aan de hand van een onafhankelijk uitgevoerd dubbelblind onderzoek bij meer dan 5.100 IT- en security professionals wereldwijd. We analyseren de data, komen met in het oog springende bevindingen en delen lessen die kunnen worden geleerd om de security in uw organisatie te maximaliseren.

Belangrijkste bevindingen

We vroegen meer dan 5.100 IT- en security professionals uit 27 landen naar de aanpak van hun organisatie van het bijwerken en integreren van security architectuur, het detecteren van/reageren op bedreigingen en hun resiliency wanneer zich een calamiteit voordoet. Ze deelden een brede reeks inzichten, problemen, strategieën en successen. We analyseerden elke respons op meerdere manieren en kwamen met belangrijkste bevindingen die hieronder zijn opgenomen.

Architectuur bijwerken en integreren

- Moderne, goed geïntegreerde IT draagt bij aan het algehele succes van programma's, meer dan enige andere security praktijk of controle.
- Nieuwere, cloudgebaseerde architecturen kunnen veel eenvoudiger regelmatig worden vernieuwd om gelijke tred te houden met de bedrijfsactiviteiten.
- Organisaties die met name producten van één leverancier gebruiken, verdubbelen de mogelijkheid tot het bouwen van een geïntegreerde technologiestack.
- Geïntegreerde security technologieën behalen zeven keer vaker hoge niveaus van process automation.

Cyberdreigingen detecteren en erop reageren

- SecOps-programma's waarbij de facetten mensen, processen en technologie alle drie sterk zijn, presteren 3,5 keer beter dan programma's met geen enkel sterk facet.
- Externe detectie-en-respons teams worden als superieur gezien, maar interne teams realiseren een kortere gemiddelde responstijd (6 in plaats van 13 dagen).
- Teams die veel gebruikmaken van threat intelligence melden twee keer zo vaak krachtige mogelijkheden voor detectie en respons te hebben.
- Automation meer dan verdubbelt de prestaties van minder ervaren mensen. Hierdoor kunnen sterke teams vrijwel zeker (95%) SecOps-succes behalen.

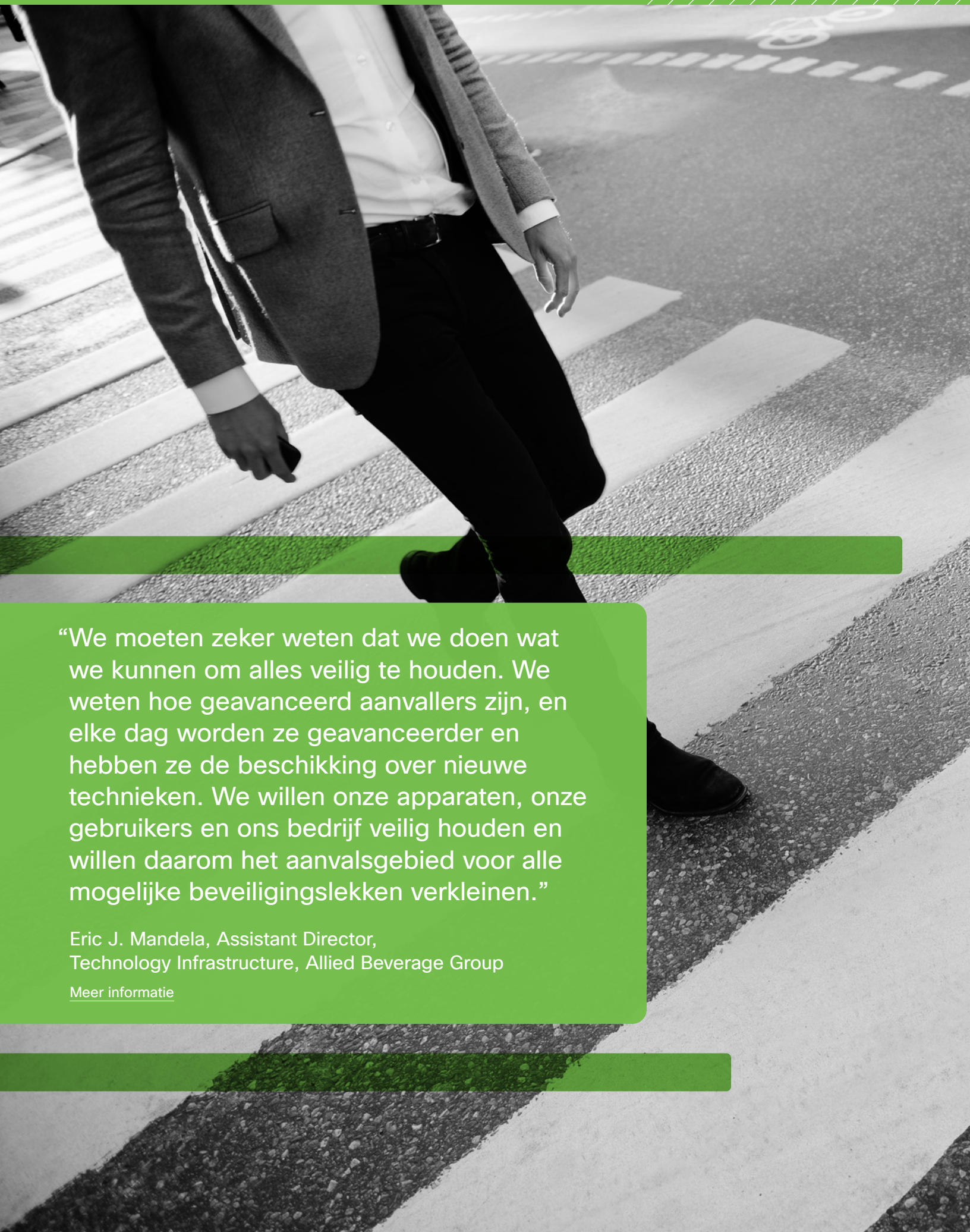
Resiliency wanneer zich een calamiteit voordoet

- Organisaties met toezicht op directieniveau van bedrijfscontinuïteit en noodherstel melden vaker (11% boven het gemiddelde) sterke programma's te hebben.
- De mogelijkheid tot business resiliency verbetert pas wanneer bedrijfscontinuïteit en noodherstel voor ten minste 80% van de cruciale systemen geldt.
- Organisaties die hun mogelijkheden tot bedrijfscontinuïteit en noodherstel regelmatig op meerdere manieren testen, zijn tot 2,5 keer vaker in staat business resiliency te garanderen.
- Organisaties die chaos engineering als standaardpraktijk toepassen, zijn twee keer zo vaak in staat hoge niveaus van resiliency te behalen.

Informatie over het onderzoek

Uitvoering	Respondenten	Analyse
Cisco heeft het onderzoeksbureau YouGov opdracht gegeven een volledig anoniem onderzoek uit te voeren op basis van een gestratificeerde aselecte steekproef. Dit is medio 2021 gebeurd.	5.123 actieve IT-, privacy- en security professionals uit 27 landen hebben deelgenomen. De demografische gegevens van de steekproef zijn opgenomen in de bijlage.	Het Cyentia Institute voerde namens Cisco onafhankelijke analyses uit van de onderzoeksdata en genereerde alle resultaten die in dit onderzoek worden gepresenteerd.

5.123 actieve IT-, privacy- en security professionals uit **27** landen hebben deelgenomen



“We moeten zeker weten dat we doen wat we kunnen om alles veilig te houden. We weten hoe geavanceerd aanvallers zijn, en elke dag worden ze geavanceerder en hebben ze de beschikking over nieuwe technieken. We willen onze apparaten, onze gebruikers en ons bedrijf veilig houden en willen daarom het aanvalsgebied voor alle mogelijke beveiligingslekken verkleinen.”

Eric J. Mandela, Assistant Director,
Technology Infrastructure, Allied Beverage Group

Meer informatie

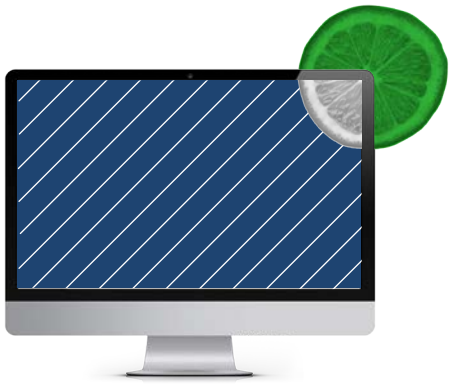
Strategieën voor proactieve vernieuwing van technologie

Uit ons vorige onderzoek bleek dat een proactieve aanpak van vernieuwing en onderhoud van superieure IT- en security technologieën meer bijdroeg aan een succesvol cyber security programma dan enige andere praktijk. Dat is niet niets gezien het feit dat alle 25 praktijken die we hebben getest algemeen worden beschouwd als 'best practices'. In dit vervolgonderzoek wilden we dan ook nagaan waardoor deze praktijk zo effectief is.

Voordat we dieper ingaan op strategieën voor de vernieuwing van technologie, kijken we eerst even naar de vernieuwing van bestaande infrastructuur. We vroegen respondenten welk percentage van hun actieve security technologieën verouderd is. Gemiddeld wordt 39% van de security technologieën die door organisaties worden gebruikt als verouderd beschouwd. Bijna 13% van de respondenten geeft aan dat ten minste 8 van de 10 security tools die ze gebruiken hun leeftijd tonen.

Alleen al dat feit verklaart veel van de voordelen die een strategie van proactieve vernieuwing van technologie biedt. Kennelijk bieden nieuwe technologieën geavanceerde mogelijkheden tegen het almaar toenemende aantal cyberdreigingen. Maar dat is niet alles. Laten we daarom verder ingaan op vragen over de data.

Gemiddeld wordt 39% van de security technologieën die door organisaties worden gebruikt als verouderd beschouwd.



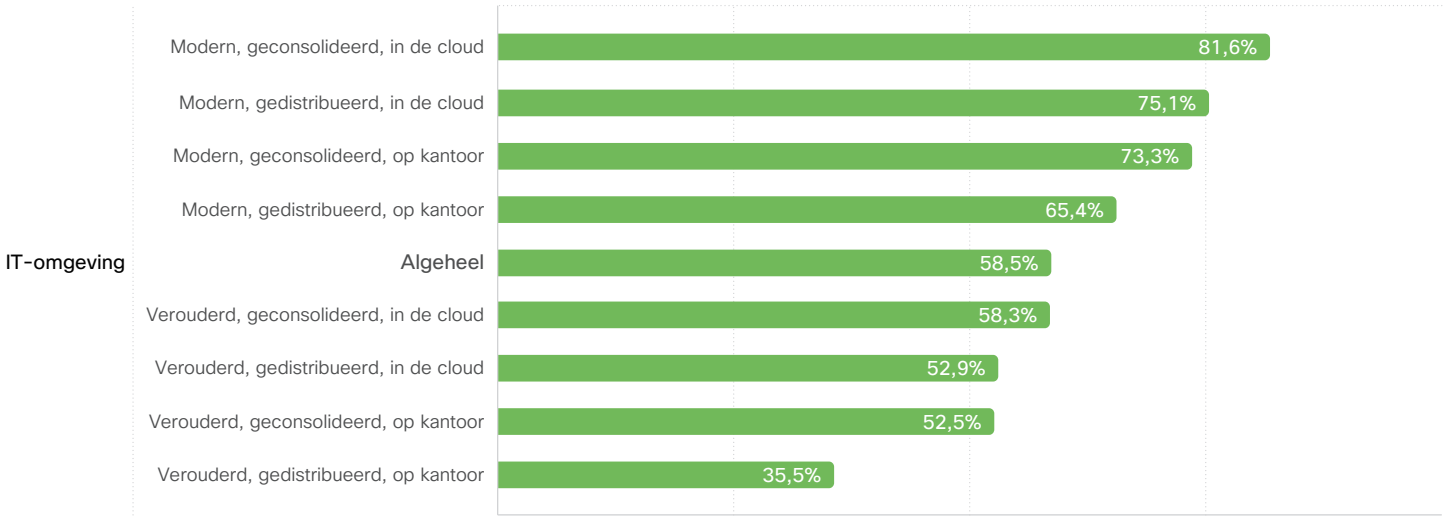
Beïnvloedt de infrastructuur initiatieven tot vernieuwing?

In het oorspronkelijke onderzoek speculeerden we dat modernere, cloudgebaseerde architecturen mogelijk effectiever zijn omdat ze gemakkelijker te beheren zijn en ingebouwde native security maatregelen hebben. Om deze hypothese te testen, vroegen we respondenten om een algemene beschrijving te geven van hun technische infrastructuur door te kiezen uit een reeks geschaalde descriptoren, zoals:

- In de cloud of op kantoor
- Modern of verouderd
- Geconsolideerd of gedistribueerd

Dragen deze architecturale eigenschappen bij aan de effectiviteit van mogelijkheden tot vernieuwing van technologie? Jazeker, zo blijkt uit afbeelding 1. **Organisaties met moderne, geconsolideerde, cloudgebaseerde architecturen melden twee keer zo vaak krachtige mogelijkheden tot vernieuwing van technologie dan organisaties met verouderde, gedistribueerde technologieën op kantoor.** Voordat u deze statistiek inzet tijdens de volgende vergadering over cloudmigratiestrategieën, moet u wel weten dat organisaties met voornamelijk kantooromgevingen nog steeds bovenmaats presteren, mits hun IT is gemoderniseerd.

Cloud-native zijn maakt het zeker gemakkelijker om uw strategie voor vernieuwing van technologie te verbeteren, maar verouderde technologieën vormen hierbij het grootste obstakel. Wanneer het vernieuwen van een oudere infrastructuur steeds moeilijker wordt, kunt u misschien beter migreren naar een nieuwe architectuur dan de oude achteraf aan te passen. Dat is natuurlijk niet altijd mogelijk of kosteneffectief bij een verouderde of kritieke infrastructuur, maar het algemene principe blijft van toepassing.

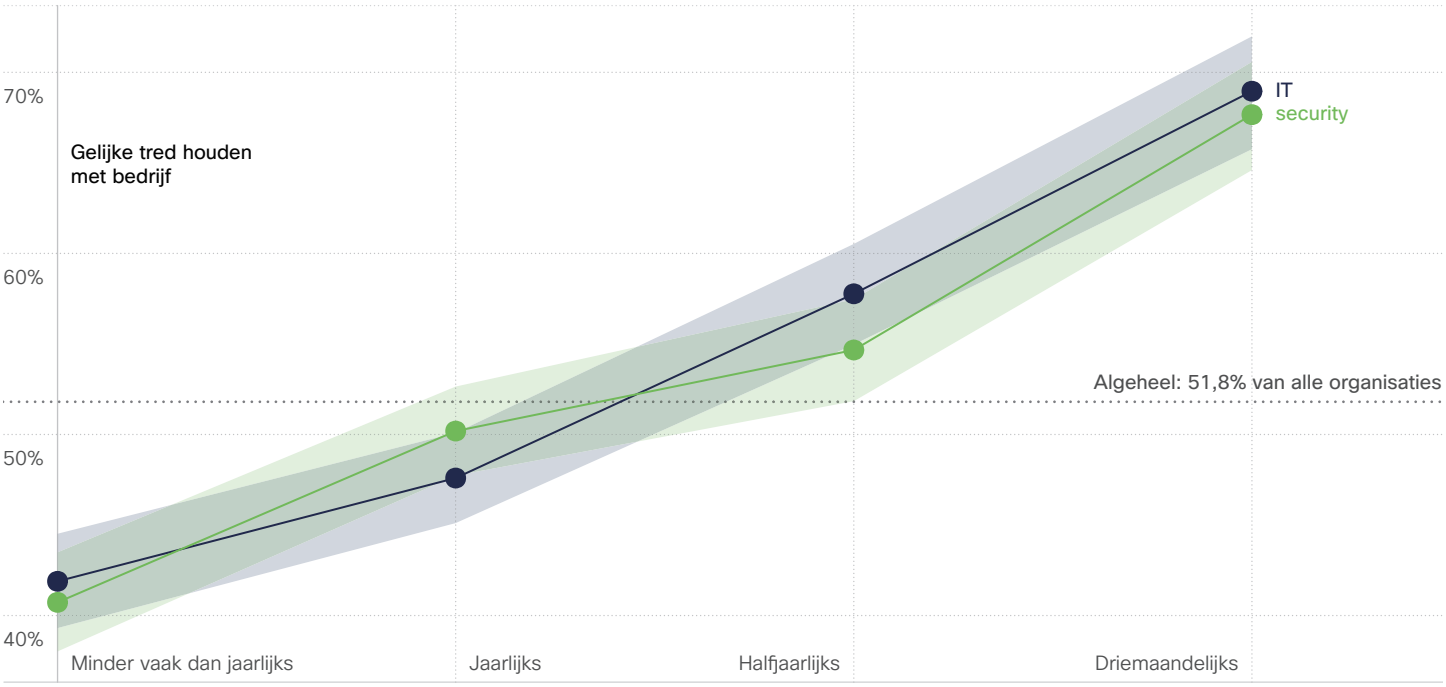


Afbeelding 1: Effect van eigenschappen van IT-architectuur op vernieuwing van technologie

81,6% van organisaties met moderne, geconsolideerde, cloudgebaseerde architecturen melden krachtige mogelijkheden tot vernieuwing van technologie

Zorgen frequente upgrades ervoor dat de security gelijke tred houdt met de bedrijfsactiviteiten?

Volgens de Security Outcomes Study 2021 correleert het resultaat sterk met een strategie van proactieve vernieuwing van technologie, zodat het security programma aan de behoeften en groei van het bedrijf kan blijven voldoen. Dat vormde zelfs de sterkst afhankelijke combinatie van praktijk en resultaat in het onderzoek.



Afbeelding 2: Effect van frequentie van vernieuwing van technologie op mogelijkheid van security programma om gelijke tred te houden met bedrijfsactiviteiten[1]

We vroegen organisaties naar de frequentie van hun IT- en security upgrades en vergeleken hun antwoorden met de aangegeven mogelijkheid van hun security programma om gelijke tred te houden met hun bedrijfsactiviteiten. Is er een relatie tussen deze twee variabelen?

Jazeker: het bleek dat naarmate upgrades frequenter worden uitgevoerd het resultaat gestaag verbeterde. **Organisaties die driemaandelijkse upgrades uitvoeren van IT- en security technologieën zijn ongeveer 30% beter in staat om gelijke tred te houden met de bedrijfsactiviteiten dan organisaties die slechts om de paar jaar een upgrade uitvoeren.** Dat lijkt dus een goed advies voor overbelaste IT-teams: blijf up-to-date.

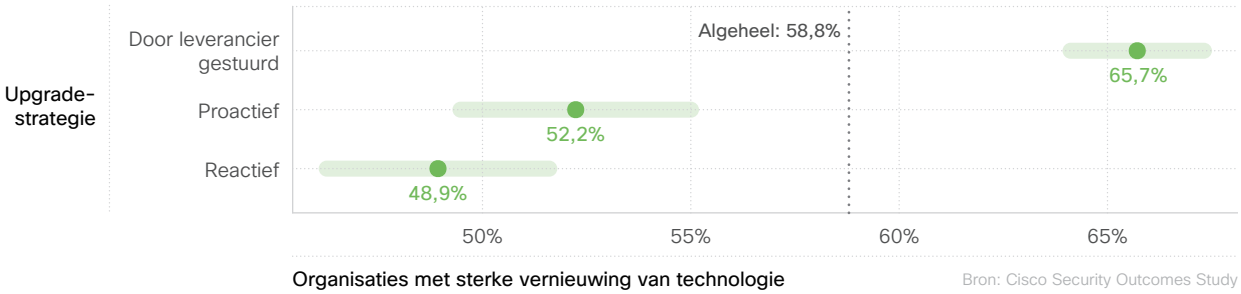
[1] In de afbeeldingen in dit rapport wordt de waarde 'Algeheel' van een bepaalde praktijk of bepaald resultaat aangegeven. Die waarde vertegenwoordigt de gemiddelde waarde bij alle respondenten die een bepaalde reeks vragen hebben beantwoord. De algehele waarde wordt ter referentie gegeven, zodat u kunt nagaan wie het beter doet dan gemiddeld en wie minder. In sommige grafieken is ook de onzekerheid aangegeven met behulp van foutbalken of gearceerde gebieden. Wanneer die gebieden de lijn met de algehele waarde overlappen, kunnen we niet aangeven dat dat specifieke aspect van een security programma enig effect heeft op het resultaat of de praktijk die we onderzoeken.

Wat (of wie) moet inspanningen op het gebied van vernieuwing van technologie stimuleren?

We hebben vastgesteld dat frequente upgrades bijdragen aan de bedrijfsresultaten, maar wat (of wie) moet ervoor zorgen dat die upgrades plaatsvinden? We vroegen de respondenten de belangrijkste drijfveren van hun organisatie tot het vernieuwen van security technologieën te selecteren, en hun antwoorden vielen in grofweg drie categorieën:

- **Door leverancier gestuurd:** Het schema wordt bepaald door een SaaS-provider of is onderdeel van een groter initiatief van een consolidatie van leveranciers (belangrijkste drijfveer)
- **Proactief:** Er wordt een vooraf bepaald schema gevolgd of er wordt een upgrade uitgevoerd wanneer nieuwe functies of use cases daarom vragen (op één na belangrijkste drijfveer)
- **Reactief:** Er wordt een upgrade uitgevoerd na een incident, wanneer technologie verouderd raakt of om aan compliance-vereisten te voldoen (minst belangrijke drijfveer)

Deze drijfveren zijn op zich interessant maar wat we echt willen weten, is of dergelijke motieven correleren met een sterke benadering van vernieuwing van technologie. Het antwoord is te zien in afbeelding 3, waaruit blijkt dat initiatieven op het gebied van vernieuwing van technologie succesvoller zijn wanneer deze door leveranciers worden uitgevoerd (of waar deze ten minste actief betrokken zijn bij de uitvoer ervan). **Minder dan de helft van de respondenten die een reactieve benadering toepassen geeft aan sterke mogelijkheden tot vernieuwing te hebben, dit in vergelijking met bijna twee derde van de respondenten die zich houdt aan de vernieuwingscycli van de leverancier.**



Afbeelding 3: Effect van belangrijkste drijfveren voor upgrades op vernieuwing van security technologie

Dit klinkt natuurlijk wat verdacht omdat we zelf leverancier zijn van IT- en security producten. Maar we hebben geen enkele invloed gehad op deze bevinding. Het onderzoek is uitgevoerd door een onafhankelijk, gerespecteerd onderzoeksbureau, de respondenten wisten niet dat Cisco het onderzoek sponsorde en de data is geanalyseerd door het vooraanstaande Cyentia Institute om te komen tot de grafiek in afbeelding 3. Bovendien zijn we bij de interpretatie van deze resultaten extra zorgvuldig te werk gegaan.

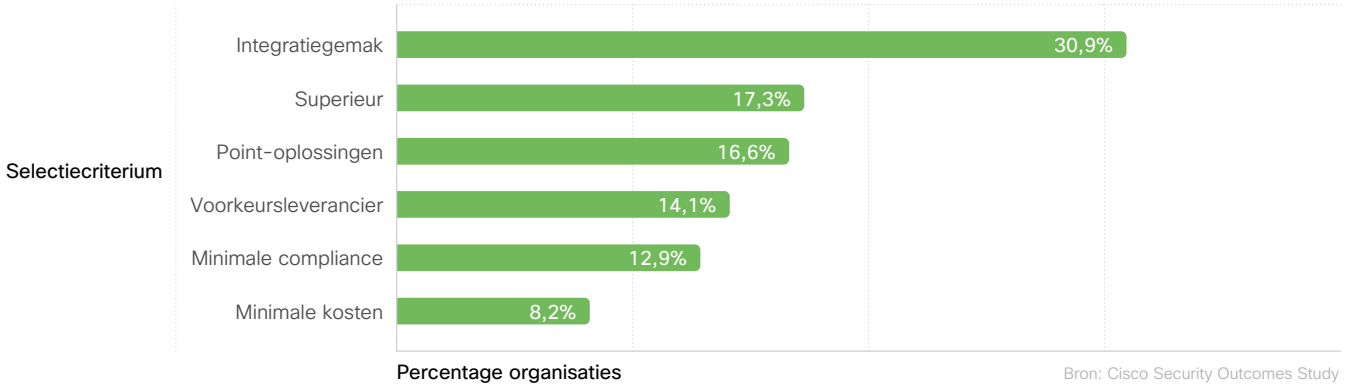
We vermoeden dat veel van de verbeteringen die worden toegeschreven aan door de leverancier gestuurde benaderingen, te maken hebben met het feit dat frequente upgrades van cloudgebaseerde architecturen/SaaS-architecturen gemakkelijker zijn uit te voeren. En de uitkomst heeft mogelijk minder te maken met geweldige leveranciers en meer met het oplossen van interne belemmeringen en politieke wirwar die vernieuwing van technologie in de weg staan.

In de woorden van Rob Base and DJ E-Z Rock, “It takes two to make a thing go right. It takes two to make it outta sight.” Het lijken wel security architecten! Zorg voor een optimale vernieuwingsstrategie door de standvastigheid van uw technologische oplossingspartners te benutten om de resultaten te verbeteren.

65,7% van de organisaties die meegaan met de vernieuwingscycli van de leverancier meldt krachtige mogelijkheden tot vernieuwing van technologie

Upgraden voor mogelijkheden of compatibiliteit?

In de vorige sectie werden de scenario's beschreven die organisaties ertoe aanzetten technologieën te upgraden. In deze sectie wordt beschreven waarom ze voor een bepaalde oplossing kiezen. In afbeelding 4 wordt aangegeven wat de respondenten vertelden over hun selectiecriteria. Goede integratie met bestaande technologie heeft duidelijk de voorkeur, gevolgd door oplossingen die superieure mogelijkheden bieden of aan bepaalde behoeften voldoen. Het minimaliseren van de kosten staat verrassend genoeg laag op de lijst.



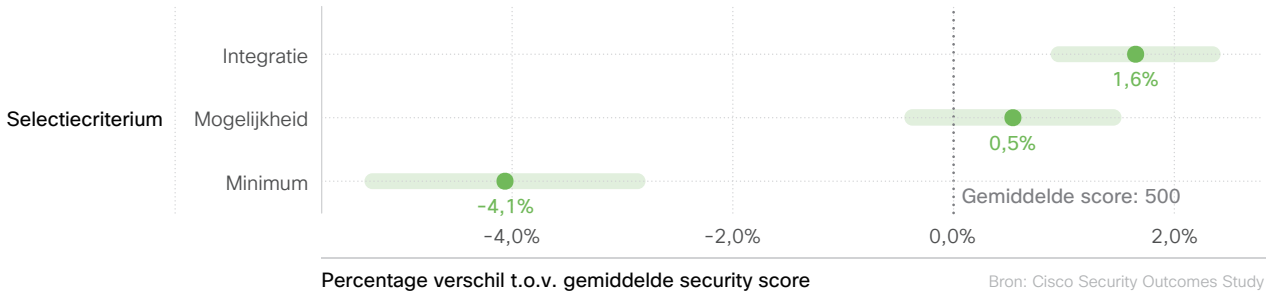
Bron: Cisco Security Outcomes Study

Afbeelding 4: Belangrijkste selectiecriteria bij vernieuwen van security producten

Dat is allemaal fijn om te weten, maar wat is het belang ervan bij het bouwen van een succesvol security programma? Om die vraag te beantwoorden, hebben we de selectiecriteria uit afbeelding 4 gegroepeerd in drie categorieën:

- **Minimum:** Minimale kostenoplossing; minimale compliance
- **Integratiegemak:** Integratie met bestaande technologie; inzet van voorkeursleveranciers
- **Mogelijkheid:** Superieur; point-oplossingen

Vervolgens hebben we deze categorieën getoetst aan de hand van een geaggregeerde score voor elke organisatie op basis van de 11 behaalde security resultaten. De absolute waarde van de score heeft geen specifieke betekenis, maar vormt een punt van vergelijking voor de verschillende strategieën voor vernieuwing van technologie. **Zoals u in afbeelding 5 kunt zien, stimuleren prioritering van integratie en mogelijkheden de resultaten meer dan het selecteren van producten om kosten te minimaliseren of te voldoen aan minimale compliance-vereisten. Maar een op integratie gebaseerde benadering is de enige die duidelijk betere resultaten oplevert dan gemiddeld.**



Afbeelding 5: Effect van selectiecriteria op algehele security score

De verschillen zijn best klein waar het het algehele succes van het programma betreft. En we zien hier waarschijnlijk een beeld van de bredere prioriteiten en praktijken van het security programma. Maar hieruit blijkt ook dat andere aspecten van belang zijn, zoals waarom we de voorkeur geven aan een bepaald product. Als u moeite heeft met het bepalen welke functies het belangrijkste zijn bij het vernieuwen of upgraden van security oplossingen, kunt u deze bevinding als redelijke rechtvaardiging beschouwen om de aandacht te richten op compatibiliteit en mogelijkheid in plaats van kostenminimalisering.

Wat is de nieuwe security score?

We vroegen respondenten in hoeverre hun organisatie succesvol was bij het behalen van 12 resultaten van hun security programma. In de eerste editie van de Security Outcomes Study werden deze gedetailleerd geanalyseerd, en enkele ervan worden ook in deze editie onderzocht. Maar we wilden ook een geaggregeerde score opnemen van de 12 behaalde security resultaten om de algehele prestaties van het security programma te bepalen. Dit is de 'security score' waarnaar in dit rapport enkele keren wordt verwezen.

Om tot deze score te komen, gebruikten we de statistische techniek Itemresponstheorie (IRT). Met deze techniek kunnen we organisaties een score geven op basis van al hun resultaten en tegelijkertijd rekening houden met het feit dan sommige resultaten lastiger te realiseren zijn dan andere. Met deze beproefde techniek worden gestandaardiseerde testscores gemaakt. De absolute waarde van de score heeft geen specifieke betekenis, maar vormt een punt van vergelijking tussen programma's.

“CISO’s moeten zowel beïnvloeders als voorlichters zijn. Om zo effectief mogelijk te zijn, moeten we in onze organisaties toonaangevende strategische beslissingen nemen. We proberen mensen ervan te overtuigen dat security belangrijk is, dat we daartoe de juiste investeringen moeten doen en dat we bij elk aspect van het bedrijf betrokken moeten zijn. Maar we moeten mensen ook voorlichten. De meeste leidinggevenden hebben geen achtergrond in security. Daarom moeten we ze bij elke stap informeren over de typen risico’s van elke beslissing die we nemen.”

Helen Patton, Advisory CISO, Cisco @CisoHelen

Luister naar Helen die vertelt over de veranderde rol van CISO’s in deze interessante aflevering van de Security Stories-podcast

Goed geïntegreerde security technologieën realiseren

Volgens onze recentste Security Outcomes Study dragen goed geïntegreerde security technologieën die effectief samenwerken met de bredere IT-infrastructuur bij aan de kans op het behalen van alle programma resultaten. We stelden een reeks vragen om meer informatie te krijgen over de factoren achter dit succes, beginnend met de intentie van integratie van security technologieën.

Volgens de respondenten is de meest gangbare motivatie voor de integratie van security technologieën het verbeteren van de efficiëntie van monitoring en auditing. Daar kunnen we ons in vinden, aangezien we maar al te bekend zijn met de frustraties die gepaard gaan met het controleren van talrijke consoles of dashboards om enig inzicht te krijgen van wat er op het netwerk gebeurt. Eenvoudigere samenwerking en automation waren ook veelgenoemde drijfveren voor de integratie van security technologieën (dat laatste komt later aan bod). We hebben deze motivaties afgezet tegen de gemelde integratieniveaus van technologie en de programmaresultaten, maar er was geen sterke correlatie. Misschien is 'wat' of 'hoe' belangrijker dan 'waarom' bij de integratie van security technologieën? Laten we hier met de volgende vragen dieper op ingaan.

Volgens de respondenten is de meest gangbare motivatie voor de integratie van security technologieën het verbeteren van de efficiëntie van monitoring en auditing.

Kopen of bouwen voor goed geïntegreerde technologie?

We weten uit het vorige onderzoek dat de integratie van security technologieën helpt bij het behalen van resultaten, maar wat is de beste manier om een verregaand geïntegreerde technologiestack te realiseren? Kant-en-klaar kopen? Zelf bouwen? Gewoon laten zoals het is? Laten we kijken wat de respondenten zeiden.

We vroegen organisaties naar hun typische benadering van integratie van security technologieën. Hun antwoorden zijn in afbeelding 6 opgenomen. **Meer dan driekwart van de respondenten gaf aan dat hun organisatie liever geïntegreerde oplossingen koopt dan ze zelf te bouwen.** Meer dan 40% van die organisaties koos voor technologieën met kant-en-klare integraties in hun bestaande infrastructuur. En meer dan 37% ging een stap verder en gaf de voorkeur aan oplossingen afkomstig van één leverancier, zodat ze native goed geïntegreerd of deel van een groter platform zijn. Net iets meer dan 20% is bereid om integraties zelf te bouwen, onder voorwaarde dat het product aan hun behoeften voldoet. Slechts enkele organisaties doen er niets aan.

Bron: Cisco Security Outcomes Study

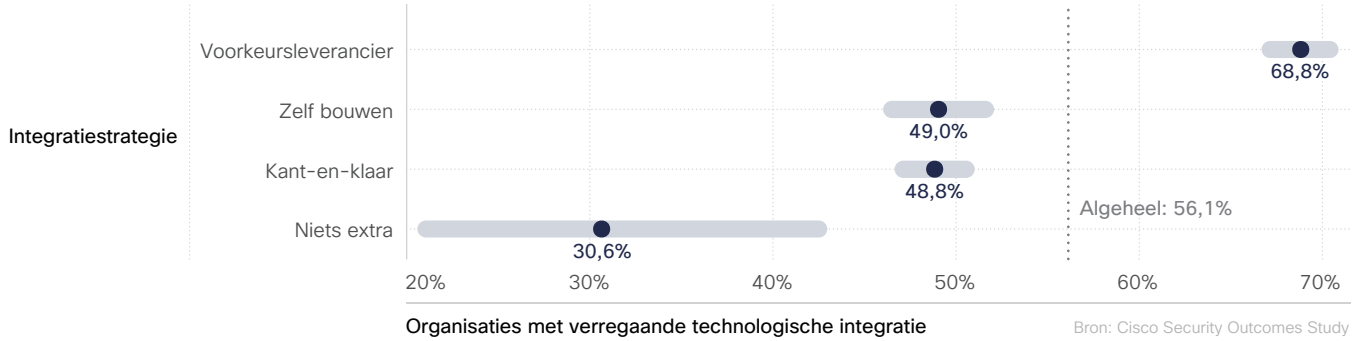
Afbeelding 6: Gangbare benaderingen van integratie van security technologieën bij alle organisaties

Meer dan **3/4** van de respondenten gaf aan dat hun organisatie liever geïntegreerde oplossingen koopt dan ze zelf te bouwen

In afbeelding 7 wordt geëvalueerd of deze benaderingen een verschil maken. Hier is opnieuw sprake van een thema dat verwijst naar de voordelen van samenwerken met leveranciers om technologie modern en goed geïntegreerd te houden. **Zoals in de grafiek te zien is, is de kans op het realiseren van goed geïntegreerde security technologieën door een voorkeursleverancier in te zetten twee keer zo groot vergeleken met een hands-off benadering (~69% tegen ~31%).** Verder blijkt uit ons onderzoek dat dit voor organisaties van alle groottes geldt, hoewel de voordelen van de inzet van een voorkeursleverancier iets groter zijn bij MKB-bedrijven dan bij grote ondernemingen.

We realiseren ons dat dit ook weer een verdacht gunstige uitkomst is voor een bedrijf met een uitgebreide, geïntegreerde security portfolio. Natuurlijk zijn we blij dat dit resultaat Cisco's strategie ondersteunt, maar dit was een dubbelblind onderzoek en we hebben de uitkomst op geen enkele manier gemanipuleerd.

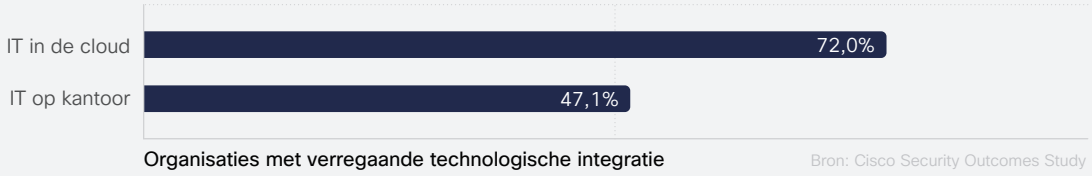
Het is niet verrassend dat er bij organisaties die niets extra's hebben gedaan om security technologieën te integreren sprake is van een selffulfilling prophecy. **We verwachten echter wel dat sommige verrast zullen zijn dat er vrijwel geen verschil is tussen bedrijven die producten met kant-en-klare integraties kopen en bedrijven die zelf integraties bouwen.** Bijna de helft (~49%) van de organisaties die één van deze benaderingen toepast, meldt verregaande integratieniveaus.



Afbeelding 7: Effect van veelvoorkomende benaderingen op integratieniveau van security technologieën

Bewolkt, met kans op integratie

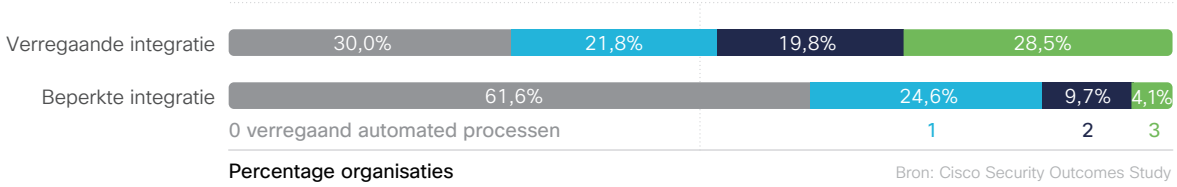
Veel organisaties geven aan dat ze worstelen met de vraag of ze in de cloud of juist op kantoor moeten beginnen met de integratie van security technologieën (of deze moeten uitbreiden). Als dit voor u geldt, dan hebben we wat data die zou kunnen helpen bij deze beslissing. Het goede nieuws is dat veel respondenten goede resultaten melden van zowel cloud- als kantooromgevingen. Het lijkt echter aanzienlijk eenvoudiger te zijn om verregaande integratie van technologie te bereiken in de cloud.



Afbeelding 8: Effect van cloud- en kantooromgevingen op integratieniveau van security technologieën

Ondersteunt integratie automation?

Zoals aan het begin van deze sectie werd aangegeven, is automation niet de belangrijkste motivatie om technologie te integreren. Toch heeft 44% van de bedrijven dit als incentive gemeld. Is er, los van motivaties, bewijs dat goed geïntegreerde technologieën daadwerkelijk betere automation van security processen mogelijk maken? Het bewijs gepresenteerd in afbeelding 9 laat zien dat dit inderdaad het geval is.



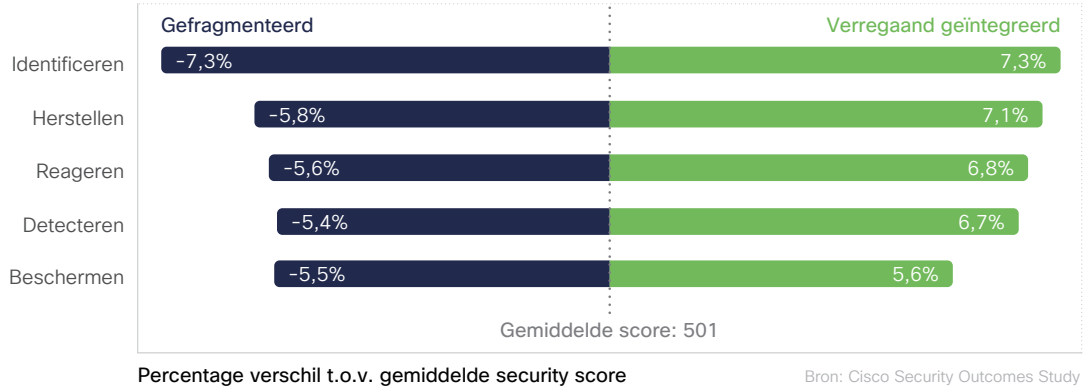
Afbeelding 9: Effect van integratie van technologieën op omvang van security process automation

De twee horizontale balken in afbeelding 9 onderscheiden organisaties op basis van hun integratieniveau van security technologieën (verregaand tegen beperkt). De gekleurde segmenten vertegenwoordigen het aantal belangrijke security processen (monitoren van gebeurtenissen, analyseren van incidenten en respons op incidenten) dat wordt ondersteund door vergevorderde automation. Het aantal organisaties zonder automation is meer dan twee keer zo groot bij de groep met beperkte integratie. **Daar staat tegenover dat organisaties met goed geïntegreerde security technologieën bijna zeven keer vaker hoge niveaus van automation behalen bij alle drie de processen (4,1% tegen 28,5%).** Dat lijkt motivatie genoeg!

Welke functies moeten worden geïntegreerd?

Vervolgens hebben we de respondenten gevraagd naar hun integratieniveau van technologieën die de vijf kernfuncties van het NIST Cybersecurity Framework (CSF) ondersteunen. Hun antwoorden varieerden van zeer gefragmenteerd (technologie in silo's die veelal in isolatie werken) tot verregaand geïntegreerd (gecoördineerde technologieën die als functionele eenheid functioneren). Op basis hiervan hebben we een model gemaakt om het effect op de algehele security score voor elke organisatie te bepalen.

De resultaten in afbeelding 10 zijn vrij consistent bij de vijf functies. **Door defragmentatie en integratie van de functionele gebieden van het NIST CSF aan te pakken, neemt het succes van een security programma toe (+11% tot ~15%).** Het antwoord op de titelvraag is dus: allemaal. Maar als u zich afvraagt waar u moet beginnen: een verregaande geïntegreerde functie 'Identify' zorgt voor de grootste impuls.



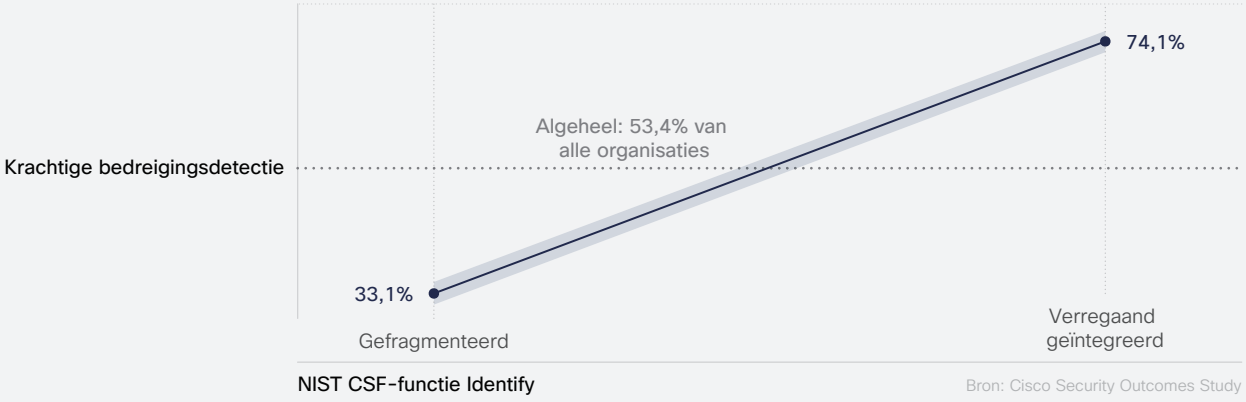
Afbeelding 10: Effect van integratie van NIST CSF-functies op algehele security score

Er is sprake van een verband tussen dit feit en wat we in de vorige sectie hebben geleerd, namelijk dat monitoring, auditing en samenwerking de belangrijkste drijfveren zijn voor het integreren van technologie. Samen lijken ze het fundamentele belang van goede zichtbaarheid van de hele onderneming te bepleiten. Het is logisch dat een gefragmenteerde aanpak van de 'ontwikkeling van organisatorisch inzicht in het beheer van cyber security risico's voor systemen, mensen, middelen, data en mogelijkheden' (CSF-bewoording) niet goed zal werken. Dit thema wordt verder versterkt in de sectie over bedreigingsdetectie en respons op incidenten.

Over integratie, identificatie en informatie

Naast de zojuist besproken grafiek wijst de data in het hele onderzoek consistent op de cruciale relatie tussen integratie, identificatie en informatie. Als u een middel of bedreiging niet kunt identificeren, weet u ook niet dat het er is en wordt u zich pas bewust van het belang van een onderbouwde verdediging als het te laat is.

Dit concept wordt goed aangegeven in afbeelding 11. We hebben het gemelde integratieniveau binnen de NIST CSF-functie 'Identify' van elke organisatie vergeleken met hun vermogen om nauwkeurig en tijdig bedreigingen te detecteren. **Organisaties met verregaand geïntegreerde systemen voor het identificeren van kritieke middelen en risico's hebben veel sterkere (+41%) mogelijkheden voor bedreigingsdetectie.** Het bestrijden van fragmentatie en het bestrijden van bedreigingen gaat dus hand in hand!



Afbeelding 11: Effect van integratie van de NIST CSF-functie Identify op bedreigingsdetectiemogelijkheden

Organisaties met verregaand geïntegreerde systemen voor het identificeren van kritieke middelen en risico's hebben

+41%

sterkere mogelijkheden voor bedreigingsdetectie

“Dankzij automation kunnen onze engineers tijdig reageren op opkomende bedreigingen. We kunnen onze aandacht nu richten op het verbeteren van de security concepten in plaats van doorlopend de regels bij te werken en het netwerk 24/7 te monitoren. Cisco gaat op zoek naar de informatie die we nodig hebben, zodat we onze infrastructuur beter kunnen beveiligen en onderhouden. Hierdoor hebben we de perfecte combinatie van menselijke en machine intelligence.”

Steve Erzberger, CTO, Frankfurter Bankgesellschaft (Schweiz) AG

Meer informatie

Mogelijkheden voor bedreigingsdetectie en respons op incidenten ontwikkelen

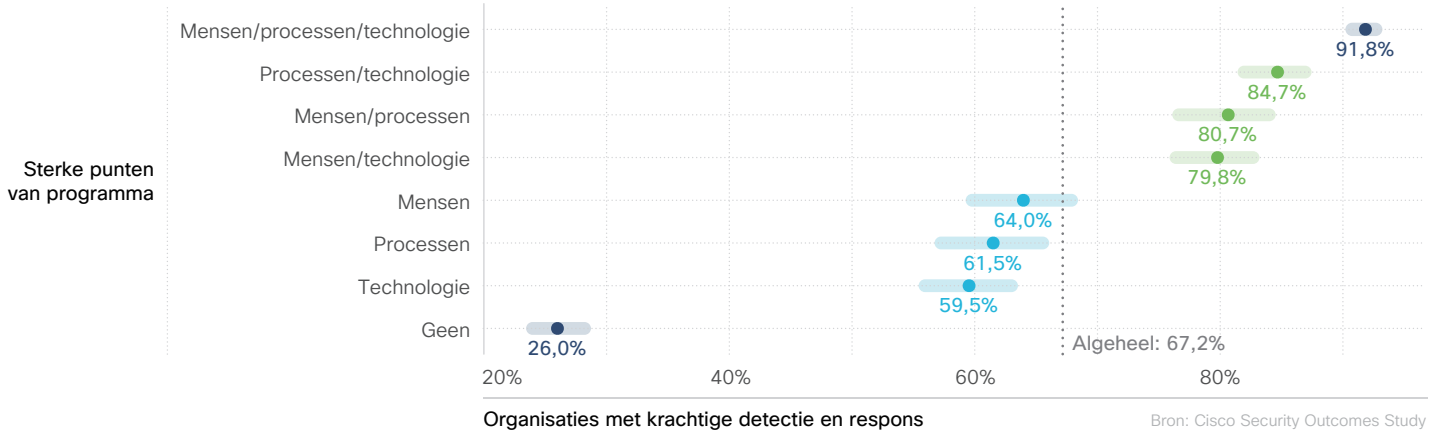
In deze sectie worden twee afzonderlijke security praktijken beschreven die beiden tot de ‘grote vijf’ behoren. Maar omdat bedreigingsdetectie en respons op incidenten (IR) vaak mensen, processen en technologieën delen onder de vlag van security activiteiten (SecOps), hebben we hierover een reeks gemeenschappelijke vragen gesteld. Daarom worden deze voor dit onderzoek binnen dezelfde sectie geanalyseerd.

Bijna alle (ongeveer 92%) organisaties waarbij de facetten mensen, processen en technologie alle drie sterk zijn, realiseren geavanceerde mogelijkheden voor bedreigingsdetectie en -respons.

Mensen, processen of technologie prioriteren?

Laten we ons onderzoek beginnen bij mensen, processen en technologie (de drie facetten). Security functies worden vaak omschreven als een combinatie van alle drie deze elementen, met name binnen het domein van bedreigingsdetectie en respons op incidenten. Maar is een van deze drie security facetten belangrijker dan de andere? U weet al wat er komt: een analyse.

Onder in afbeelding 12 ziet u dat slechts zo'n kwart van de organisaties met programma's met geen enkel sterk facet vertrouwen hebben in hun SecOps. Door een van de facetten – mensen, processen of technologie – te versterken, stijgt dat percentage tot zo'n 60% of 64%, afhankelijk van het betreffende facet. Versterking van het facet mensen lijkt het voordeel iets meer te vergroten, maar de overlappende betrouwbaarheidsintervallen duiden op de nodige onzekerheid. Het gaat erom dat elk van deze facetten een goed startpunt vormt voor het realiseren van betere detectie- en responsmogelijkheden.



Afbeelding 12: Effect van sterke facetten mensen, processen en technologie op mogelijkheden voor bedreigingsdetectie en respons op incidenten

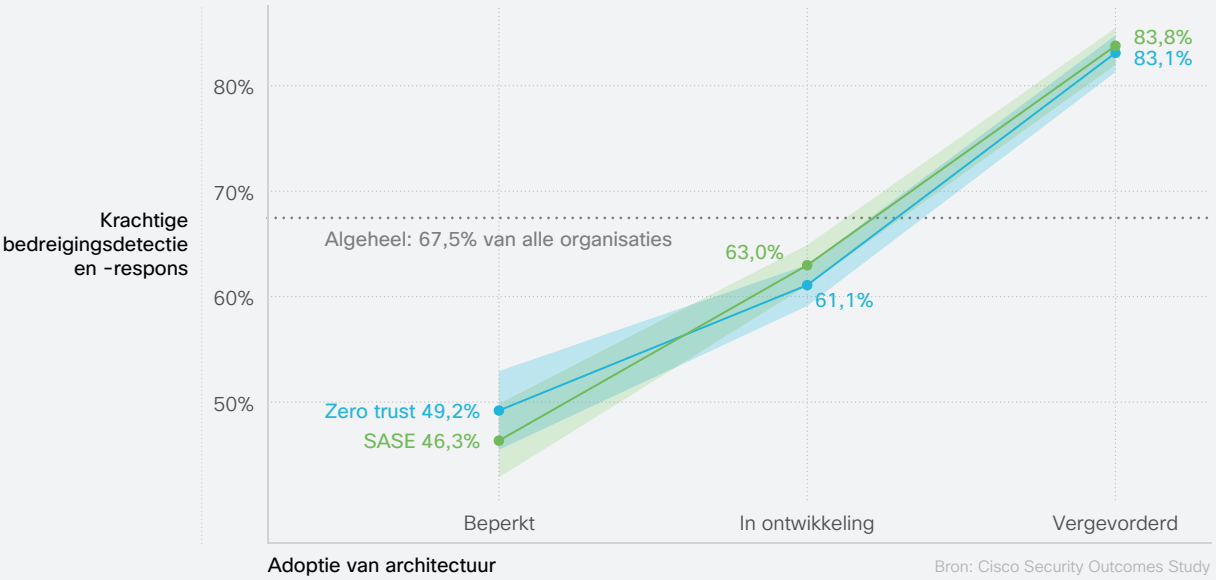
Verder naar boven in afbeelding 12 is te zien dat SecOps-programma's die op het gebied van twee facetten goed presteren duidelijk boven het gemiddelde uitkomen. Deze verbeteren de mogelijkheden met ongeveer 15% tot 20% vergeleken met programma's die slechts op het gebied van één facet goed presteren. Het maakt hierbij niet echt uit welke combinatie van mensen, processen en technologie er wordt gekozen. Als maar in elk geval twee van deze facetten worden versterkt. Het is goed om te weten dat u keuzevrijheid heeft voor wat betreft de invulling van de SecOps-roadmap van uw organisatie.

Dit brengt ons bij de topprogramma's in afbeelding 12 die erin slagen om alle drie facetten van SecOps te bewerkstelligen. **Bijna alle (ongeveer 92%) organisaties waarbij de facetten mensen, processen en technologie alle drie sterk zijn, realiseren geavanceerde mogelijkheden voor bedreigingsdetectie en -respons.** Dat is 3,5 keer hoger dan SecOps-programma's die bij geen van de drie facetten goed presteren! Begin dus waar u de meeste vooruitgang kunt boeken, maar stop niet totdat u alle drie facetten heeft gerealiseerd.

Organisaties met sterke facetten mensen, processen en technologie ervaren **3,5x** betere bedreigingsdetectie en -respons dan organisaties waar deze facetten minder sterk zijn

Zorgen zero trust en SASE voor betere SecOps?

We begrijpen dat abstracte beschrijvingen als ‘sterke technologie’ het lastig maken om concrete conclusies uit de bovenstaande bevindingen te trekken. Daarom hebben we enkele vervolgvragen gesteld over specifieke architecturen. We hebben respondenten gevraagd naar hun adoptie van zero trust en Secure Access Service Edge (SASE) om een beter beeld te krijgen van de manier waarop deze benaderingen de mogelijkheden voor bedreigingsdetectie en respons op incidenten beïnvloeden (en daarmee de resultaten van security programma’s).



Bron: Cisco Security Outcomes Study

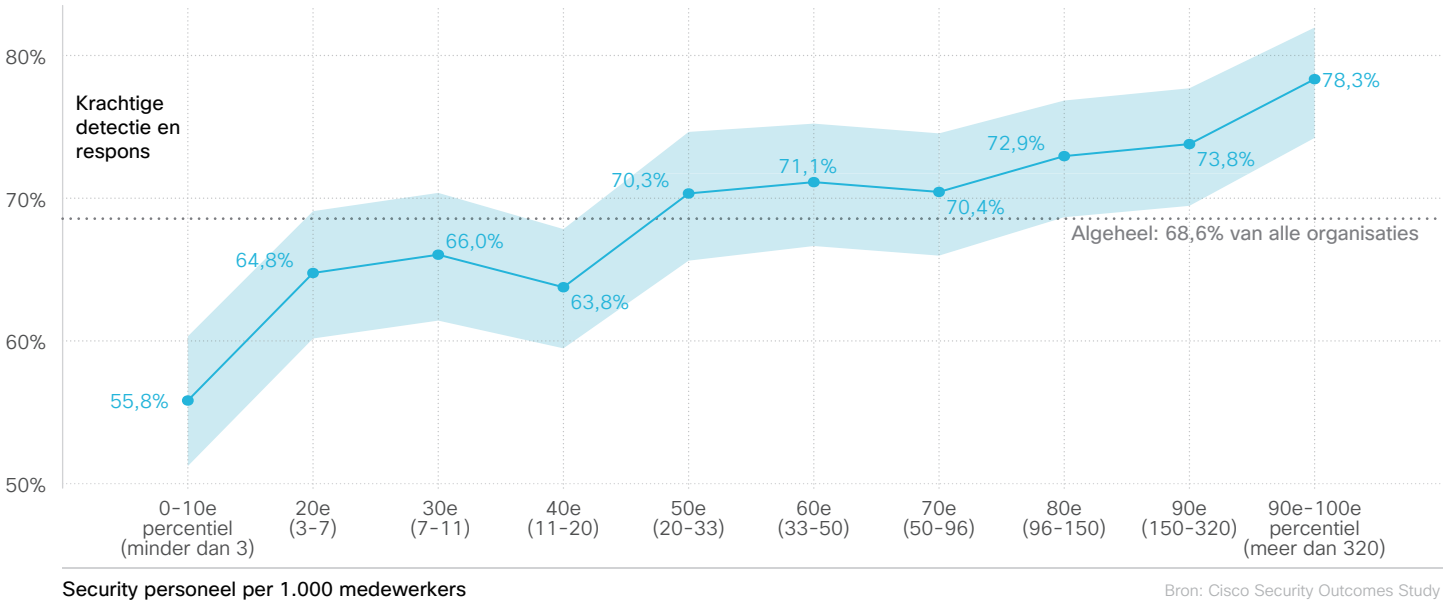
Afbeelding 13: Effect van architecturen met zero trust en SASE op mogelijkheden voor bedreigingsdetectie en respons op incidenten

Organisaties die aangeven vergevorderde implementaties van zero trust of SASE te hebben, melden 35% vaker dan organisaties met beginnende implementaties een sterke SecOps te hebben. Deze resultaten ondersteunen het bewijs dat we eerder hebben gedeeld over de vele voordelen van moderne architecturen voor cyber security programma’s.

Betekent een grotere personeelsbezetting ook minder zorgen?

We weten dat goede mensen belangrijk zijn voor het realiseren van krachtige mogelijkheden voor bedreigingsdetectie en respons op incidenten. Is het echter voor organisaties beter om zich te richten op het toevoegen van meer mensen of op het verbeteren van de vaardigheden van de mensen die ze al hebben? Het een hoeft het ander natuurlijk niet uit te sluiten, maar de vraag blijft of we bewijs kunnen vinden voor wat er belangrijker is voor de ontwikkeling van succesvolle SecOps-teams: kwantiteit of kwaliteit?

Om hierop antwoord te geven, hebben we eerst voor alle organisaties de verhouding van SecOps-medewerkers ten opzichte van het totale aantal medewerkers berekend. Dat getal hebben we vervolgens vergeleken met de gemelde sterkte van detectie- en responsmogelijkheden. Afbeelding 14 laat de uitkomst van deze berekeningen zien. Hoewel de vraag van kwantiteit of kwaliteit niet volledig wordt beantwoord, biedt deze wel enkele inzichten.



Bron: Cisco Security Outcomes Study

Afbeelding 14: Effect van verhouding van security personeel ten opzichte van totale aantal medewerkers op mogelijkheden voor bedreigingsdetectie en respons op incidenten

Het eerste inzicht is dat de verhouding van security personeel niet correleert met betere bedreigingsdetectie en -respons. Organisaties met de hoogste verhouding melden net iets meer dan 20% vaker dat ze over sterkere mogelijkheden beschikken dan organisaties met de laagste verhouding. Maar ziet u hoe de gestippelde lijn in afbeelding 14, die het totale gemiddelde aangeeft, door een groot gedeelte van het gearceerde betrouwbaarheidsinterval loopt? Dat betekent dat het voor organisaties die niet aan de extreme uiteinden van de personeelsschaal staan (de meerderheid) even waarschijnlijk is dat ze melden sterke SecOps-programma's te hebben.

Wat wil dit zeggen? We kunnen met vertrouwen stellen dat organisaties met enorme security teams aanzienlijk vaker sterke mogelijkheden voor detectie en respons realiseren dan organisaties met een beperkt aantal security medewerkers. Maar alleen een grotere personeelsbezetting maakt geen einde aan SecOps-zorgen en is ook geen garantie voor succes. Zelfs de verschillen tussen de grootste en kleinste personeelsverhouding verklaren ook niet de prestatievergroting die het gevolg is van een sterk facet 'mensen' in de vorige sectie. **We kunnen enkel afleiden dat kwaliteit even belangrijk zo niet belangrijker is dan kwantiteit als het aankomt op het creëren van sterke teams voor bedreigingsdetectie en -respons.**

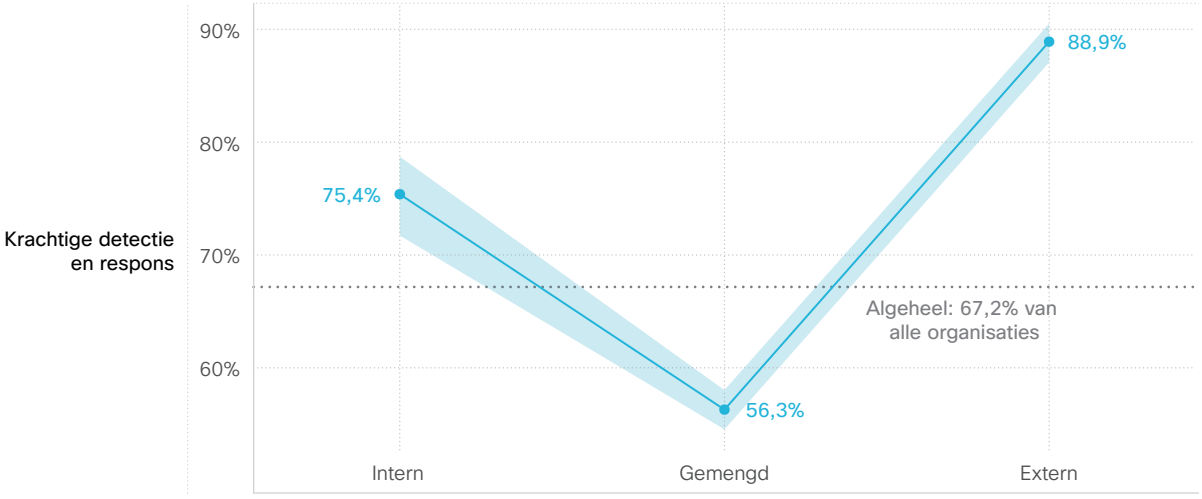
Security teams kampen nog steeds met ernstige personeelstekorten.

Door te kleine teams en toenemende bedreigingen hebben veel cyber security professionals last van extreme stress en een burn-out. Welke proactieve maatregelen kunnen we nemen om hun welzijn te vergroten? In dit e-book hebben we marktleiders en professionals gevraagd hun inzichten en verhalen te delen over het bevorderen van de geestelijke gezondheid.

SecOps-personeel: van u, van mij of van ons?

Het succes van SecOps draait dus niet alleen om personeelsbezetting, maar beïnvloeden personeelsmodellen de resultaten ook? Is het beter om de verantwoordelijkheden op het gebied van bedreigingsdetectie en -respons extern (via uitbesteding), intern of gemengd te regelen? Laten we kijken hoe de data deze vraag beantwoordt. Maar wees gewaarschuwd, er valt in dit geval voor beide kanten iets te zeggen.

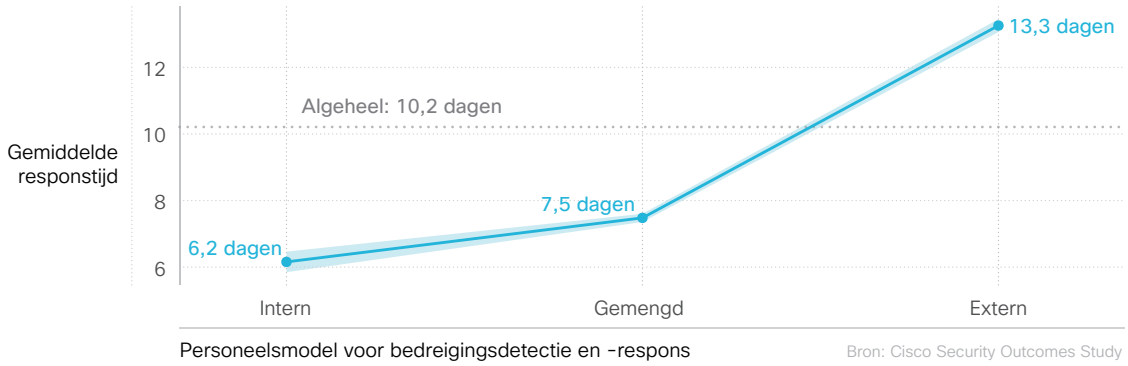
We hebben de respondenten gevraagd naar hun personeelsmodellen en deze vervolgens vergeleken met de waardering van hun detectie- en responsmogelijkheden. **Zoals u in afbeelding 15 kunt zien, meldden organisaties met overwegend interne of externe teams vaker dan organisaties met een gemengd personeelsmodel sterke SecOps-programma's te hebben (respectievelijk +20% en 30%).** Aangezien de meeste organisaties aangaven een gemengd model te gebruiken, leek het ons de moeite waard om hier vanuit een ander perspectief naar te kijken voordat we deze als een mislukking beschouwen enkel en alleen omdat de enquête dit resultaat lijkt uit te wijzen.



Afbeelding 15: Effect van personeelsmodellen op veronderstelde mogelijkheden voor bedreigingsdetectie en respons op incidenten

Organisaties met overwegend interne of externe teams hebben **20 tot 30%** vaker dan organisaties met een gemengd personeelsmodel sterke SecOps-programma's

We vroegen de respondenten de veronderstelde sterkte van hun detectie- en reponsmogelijkheden in te schatten en hebben daarnaast ook geprobeerd meer objectieve meetcriteria te verkrijgen ter vergelijking. Een van deze meetcriteria is de gemiddelde responstijd (MTTR) of de gemiddelde tijd tot het herstellen of inperken van een security incident. In onze achtergrondanalyse, buiten dit rapport om, komen deze meetcriteria vaak grotendeels overeen met de subjectieve beoordelingen. Maar de twee perspectieven spraken elkaar in dit geval tegen, zoals duidelijk wordt uit afbeelding 16.



Afbeelding 16: Effect van personeelsmodellen op gemiddelde responstijd op security incidenten[2]

Op basis van afbeelding 16 blijkt dat organisaties met interne teams voor bedreigingsdetectie en -respons een MTTR hebben die minder dan de helft korter is van die van organisaties die uitbesteden (ongeveer 6 in plaats van 13 dagen). Organisaties met hybride personeelsmodellen vallen in het midden (ongeveer 8 dagen) en hebben een MTTR die net zo lang is als bij interne teams maar veel korter dan bij organisaties met voornamelijk externe modellen.

Hier is wel enige sprake van een dilemma. Welke maatregel (perspectief tegen meetcriteria) is juist en belangrijker nog, welke moet worden toegepast om tot onderbouwde beslissingen te komen? We blijven hier opzettelijk vaag en stellen dat het 'beide' en 'geen van beide' is (we volgen hierbij gewoon de tegenstrijdige aard van de data).

Herstel omvat natuurlijk veel elementen en afhankelijkheden. Organisaties zijn mogelijk afhankelijk van een leverancier die een patch/bug fix moet leveren om een kwetsbaarheid te verhelpen. Die patch moet dan vervolgens eerst in een testomgeving worden gebruikt voordat deze in de productieomgeving wordt geïmplementeerd. Er zijn dus verschillende schijven bij betrokken.

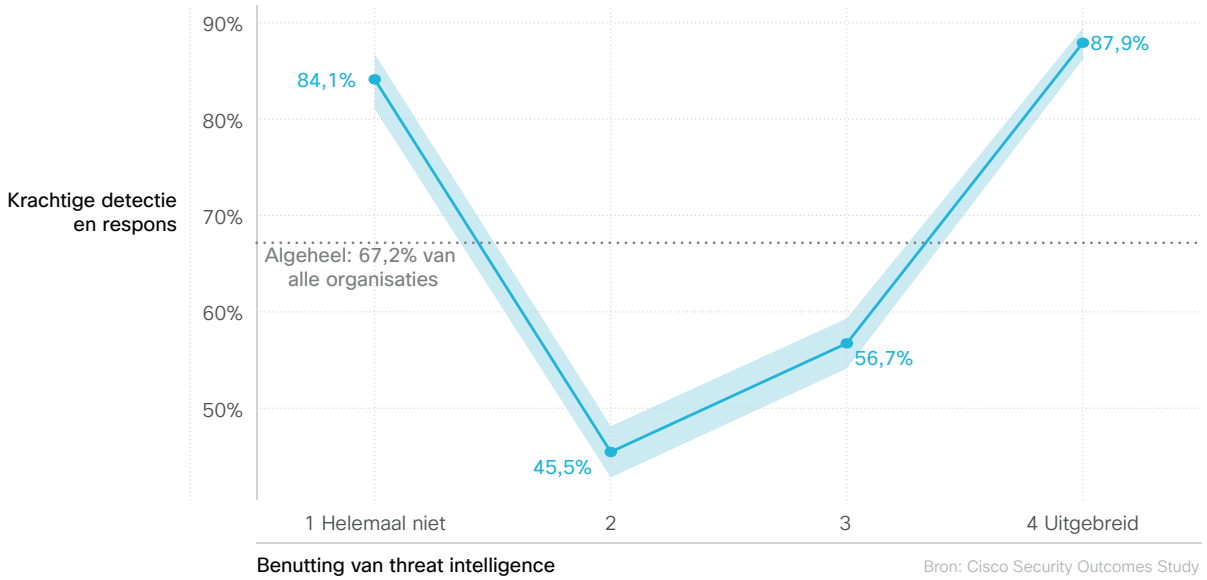
Het is lastig om hier echt een goed beeld van te krijgen. Misschien was het verzamelen van meetcriteria via een onderzoek misleidend. Misschien verschilt de waardering van MTTR en van mogelijkheden dusdanig dat het mogelijk is om een algeheel 'sterk' detectie- en responsprogramma te hebben, maar toch een lagere herstelsnelheid. Misschien zijn die programma's langzamer omdat ze grondiger werken. Misschien vereist het coördineren van extern personeel meer tijd. Misschien is er sprake van een gevoel van vertrouwen omdat 'we betalen de deskundigen dit te toen en zij zorgen dat alles goed verloopt'. Misschien is er sprake van een SecOps-versie van het Dunning-Krugereffect. Het is waarschijnlijk een combinatie van dit alles en meer. En daarom is het raadzaam een discussie op gang te brengen aan de hand van deze sectie in plaats van beslissingen te nemen.

[2] We gebruiken het geometrische gemiddelde in deze grafiek omdat die de 'typische' waarde beter vertegenwoordigt. De gemelde MTTR was doorgaans korter dan 2 tot 3 weken, maar enkele respondenten gaven maanden (of zelfs jaren) aan. Het geometrische gemiddelde vertegenwoordigt de 'typische' waarde beter, omdat dit niet wordt vertekend door uitermate hoge waarden.

Is het slim om intelligence in te zetten?

We gaan in deze sectie uit van het Dunning-Krugereffect. We vroegen de respondenten naar het gebruik van cyber threat intelligence in hun SecOps-programma. De meeste organisaties (85%) gaven aan intelligence enigszins in te zetten, maar minder dan een derde (31%) gaf aan intelligence uitgebreid toe te passen. Leidt dat tot betere, slimmere en snellere bedreigingsdetectie en -respons? Kijk eens naar afbeelding 17.

Vreemd genoeg presteren de meeste organisaties die helemaal geen threat intelligence gebruiken best wel goed. Het oude gezegde 'onwetendheid is een zegen' lijkt hier opgang te doen, aangezien bij iets verder kijken blijkt dat deze veronderstelling niet klopt (van ongeveer 84% vertrouwen naar 46%). **Organisaties die uitgebreid gebruikmaken van threat intelligence melden bijna twee keer zo vaak krachtige mogelijkheden van detectie en respons te hebben dan organisaties die intelligence minder inzetten. En in een voorbeeld waarbij de waardering van mogelijkheden en meetcriteria overeen komen, realiseren organisaties die meer intelligence inzetten MTTR's die bijna de helft korter zijn dan die bij organisaties die geen gebruikmaken van intelligence.**



Bron: Cisco Security Outcomes Study

Afbeelding 17: Effect van inzet van intelligence op mogelijkheden voor bedreigingsdetectie en respons op incidenten

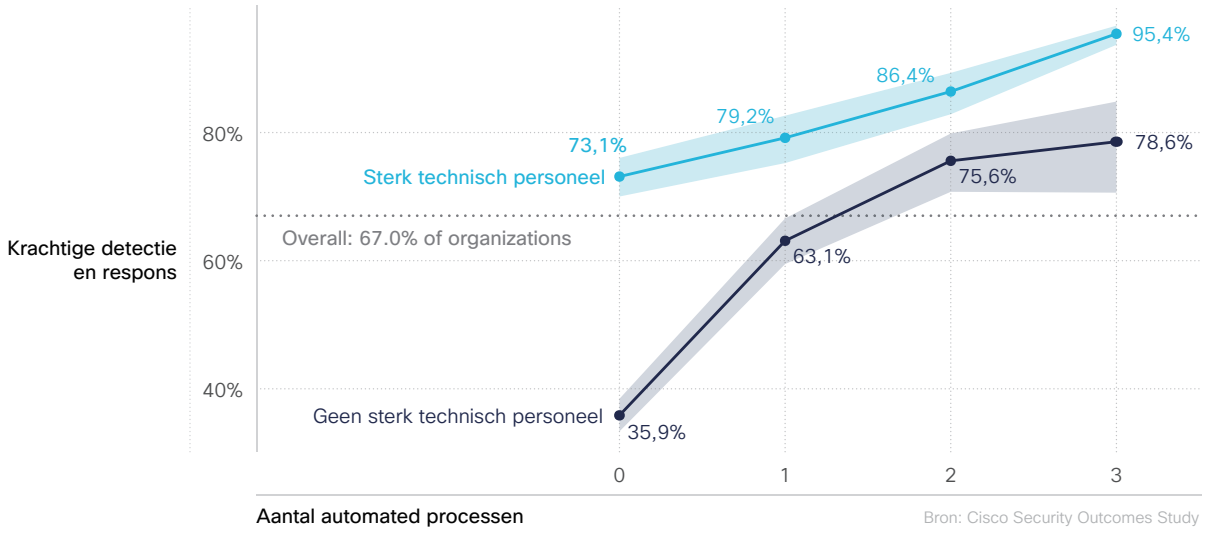
Daniel Kahneman, psycholoog en bestsellerschrijver, heeft ooit gezegd "we zijn blind voor onze blindheid. We hebben geen weet van hoe weinig we weten." Uit afbeelding 17 zou kunnen worden geconcludeerd dat zodra organisaties iets weten van de bedreigingen waarmee ze te maken hebben, ze realiseren dat er veel is dat ze niet weten. Veel uitgebreider gebruik van threat intelligence begint met het kweken van vertrouwen, maar dan nu met minder blindheid.

Organisaties die uitgebreid gebruikmaken van threat intelligence hebben bijna **2x** zo vaak krachtige mogelijkheden voor detectie en respons

Vormt automation een vervanging voor mensen?

Bij het lezen van deze titel gaat u er mogelijk vanuit dat dit een retorische vraag is. Maar dat is het niet. Met het risico dat de hele security community over ons heen valt, durven we op basis van de data te stellen dat automation inderdaad mensen kan vervangen. Maar lees verder voordat u besluit dit rapport te verwijderen en ons toe te voegen aan uw lijst met geblokkeerde contactpersonen.

In afbeelding 18 zijn elementen opgenomen die u in vorige grafieken heeft gezien: security personeel en automation. Op de twee lijnen worden verschillende typen SecOps-programma's vergeleken. De eerste lijn (donkerblauw) vertegenwoordigt organisaties die GEEN sterk facet mensen hebben. De tweede lijn (lichtblauw) vertegenwoordigt organisaties die dat WEL hebben. In beide scenario's wordt van links naar rechts het effect van toenemende automation niveaus op mogelijkheden voor bedreigingsdetectie en -respons op incidenten getoond.



Bron: Cisco Security Outcomes Study

Afbeelding 18: Effect van mate van personeelsbezetting en automation op mogelijkheden voor bedreigingsdetectie en respons op incidenten

We beginnen met de oranje lijn. Slechts een derde van de organisaties zonder sterk security personeel en waar geen belangrijke processen automated zijn, meldt sterke mogelijkheden voor detectie en respons. Wanneer een van de drie procesgebieden waarnaar we vroegen (monitoring van bedreigingen, analyse van gebeurtenissen en respons op incidenten) automated is, neemt dat aantal behoorlijk toe. Wanneer twee van die procesgebieden automated zijn, neemt de waarde nog meer toe. Wanneer ze alle drie automated zijn, verdubbelen alleen al de prestaties van minder ervaren personeel. **Meer dan driekwart van de SecOps programma's zonder een sterke personeelsbezetting is nog steeds in staat robuuste mogelijkheden te realiseren bij een hoge mate van automation.**

Volg nu de donkerblauwe lijn vanaf het meest rechtse punt naar het eerste punt van de lichtblauwe lijn. Ziet u de implicatie? **Een SecOps-programma met een zwakkere personeelsbezetting en geavanceerde automation doet het bijna net zo goed als een programma met een sterkere personeelsbezetting en weinig automation.** Anders gezegd: sterke automation kan een vervanging zijn voor sterk personeel. We zeiden toch al dat we niet logen!

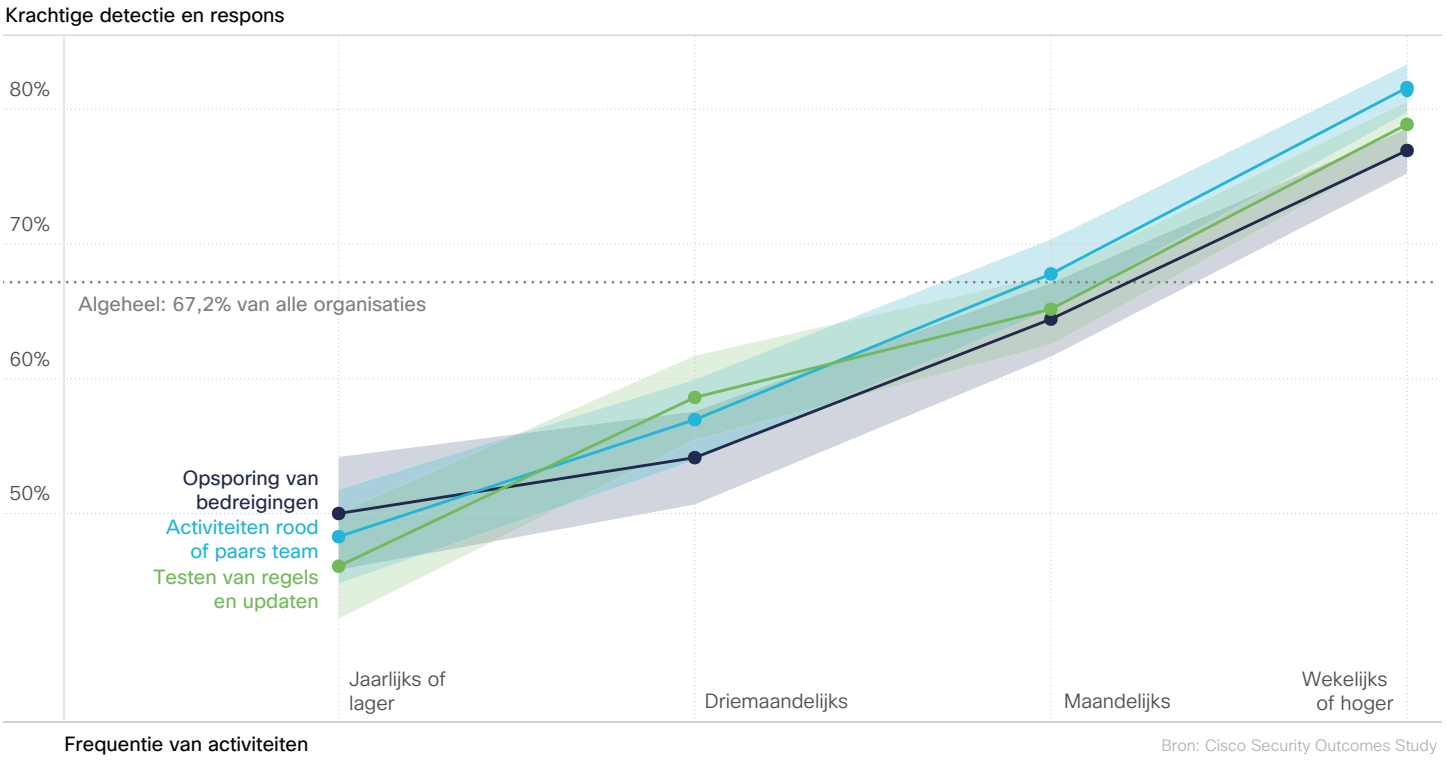
Maar mens/machine vormt niet de belangrijkste les uit afbeelding 18. Door de blauwe lijn te volgen langs opeenvolgende maten van automation wordt onderbouwing gegeven aan het advies om beide doelstellingen na te streven. Security programma's met zowel een krachtig team als automation van belangrijke processen voor bedreigingsdetectie en -respons garanderen bijna (meer dan 95%) het succes van SecOps. Gebruik automation dan ook niet als vervanging van getalenteerde medewerkers. Zet automation in om talent te ondersteunen, zodat ze zich kunnen richten op activiteiten met hoge prioriteit.

Hoe vaak moet u tweaken, hacken en opsporen?

Er zijn veel terugkerende activiteiten die potentieel de programma's voor bedreigingsdetectie en -respons kunnen verbeteren. Tijdens een informele enquête werden drie activiteiten met name aanbevolen:

- Detectieregels en use cases testen en bijwerken
- Proactief tekenen van schadelijke activiteit opsporen
- Activiteiten met rode en/of paarse teams uitvoeren

We vroegen de respondenten hoe vaak hun organisaties deze activiteiten uitvoeren en zetten het resultaat vervolgens af tegen de gemelde sterkte van mogelijkheden voor bedreigingsdetectie en -respons. De trend die uit afbeelding 19 blijkt is kristalhelder.



Afbeelding 19: Effect van frequentie van activiteiten op mogelijkheden voor bedreigingsdetectie en respons op incidenten

Testen en bijwerken van regels, activiteiten met rode en/of paarse teams en bedreigingsopsporing volgen alle een vergelijkbaar traject. Hoe vaker ze worden uitgevoerd, hoe beter dat is voor SecOps-programma's. **Organisaties die deze minimaal op wekelijkse basis uitvoeren, ervaren een prestatievergroting van zo'n 30% in vergelijking met organisaties die dat jaarlijks of minder vaak doen.** Hoe vaak zou uw organisatie de activiteiten moeten uitvoeren? Het korte antwoord is: hoe vaker hoe beter.

Organisaties die deze minimaal op wekelijkse basis uitvoeren, ervaren zo'n **30%** hogere prestaties

“Security verandert doorlopend en we moeten deze security trends volgen. Voorheen verloren we veel tijd bij het oplossen van security problemen en incidenten. Nu we het proces hebben vereenvoudigd en tijd hebben bespaard via investeringen kunnen we de nieuwe security trends volgen en nieuwe security oplossingen integreren voor een veiligere infrastructuur van ons onderwijsnetwerk.”

Bahruz Ibrahimov, Senior Information Security Engineer, AzEduNet

Meer informatie

Snel noodherstel en veerkracht garanderen

Het is interessant om te zien hoe de prioriteit van verschillende aspecten van cyber security in de loop der tijd verandert. Nadat datalekken en cyber spionage jarenlang de boventoon voerden, treden momenteel bedrijfscontinuïteit en noodherstel (BCDR) weer meer op de voorgrond. En daar is een goede reden voor. Ongeremde ransomware, uitval van grote hostingproviders, enzovoort hebben geleid tot belangrijke strategiewijzigingen om resiliency te garanderen met het oog op meedogenloze bedreigingen.

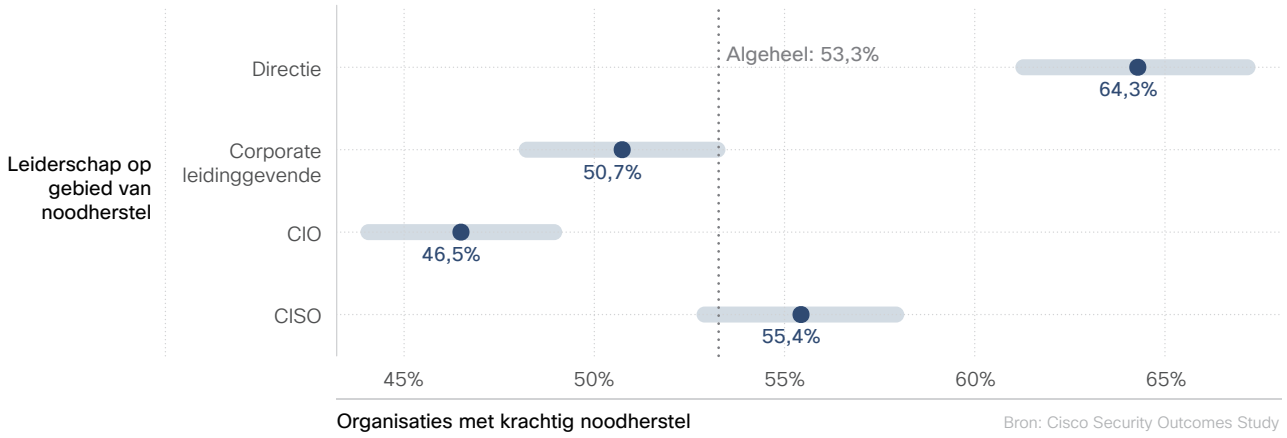
In de Security Outcomes Study 2021 werd snel noodherstel aangemerkt als het op drie na belangrijkste aspect van een succesvol cyber security programma. Er was sprake van duidelijke correlaties met alle 11 resultaten, op een na (security cultuur). Laten we met dat in gedachten strategieën voor het maximaliseren van de effectiviteit van deze praktijk en het garanderen van resiliency bekijken.

Ongeremde ransomware, uitval van grote hostingproviders, enzovoort hebben geleid tot belangrijke strategiewijzigingen om resiliency te garanderen met het oog op meedogenloze bedreigingen.

Is voor noodherstel toezicht op directieniveau vereist?

We vroegen ons af wie het uiteindelijke toezicht heeft op mogelijkheden voor noodherstel. Het blijkt dat bij telkens ongeveer een kwart van de organisaties verantwoording voor BCDR wordt afgelegd aan de CIO, CISO en twee typen niet-IT'ers onder de corporate leidinggevenden. Zichtbaarheid op directieniveau komt iets minder vaak voor, maar toch nog bij 18% van de organisaties in ons onderzoek.

Toen we deze antwoorden vergeleken met de beoordeling van elke respondent van hun BCDR-processen, bleek dat toezicht meer is dan een vorm van nieuwsgierigheid. **Zoals in afbeelding 20 te zien is, melden organisaties met toezicht op directieniveau van BCDR-processen vaker (11% hoger dan gemiddeld) dat ze sterke programma's hebben.** Organisaties waar de eindverantwoordelijkheid voor BCDR bij de CIO ligt, scoren het laagst en liggen aanzienlijk onder het gemiddelde.



Afbeelding 20: Effect van organisatorisch toezicht op hoog niveau op mogelijkheden voor noodherstel

Er zijn veel plausibele verklaringen voor de resultaten in afbeelding 20. We vermoeden dat organisaties die bij de directie verantwoording afleggen over noodherstel meer zorgen hebben over operationele risico's en resiliency. Die zorgen vertalen zich waarschijnlijk in strakker toezicht, sterkere ondersteuning en hogere budgetten. Als uw organisatie dus problemen heeft met mogelijkheden voor noodherstel, is het wellicht verstandig om dit top-down en niet bottom-up aan te pakken.

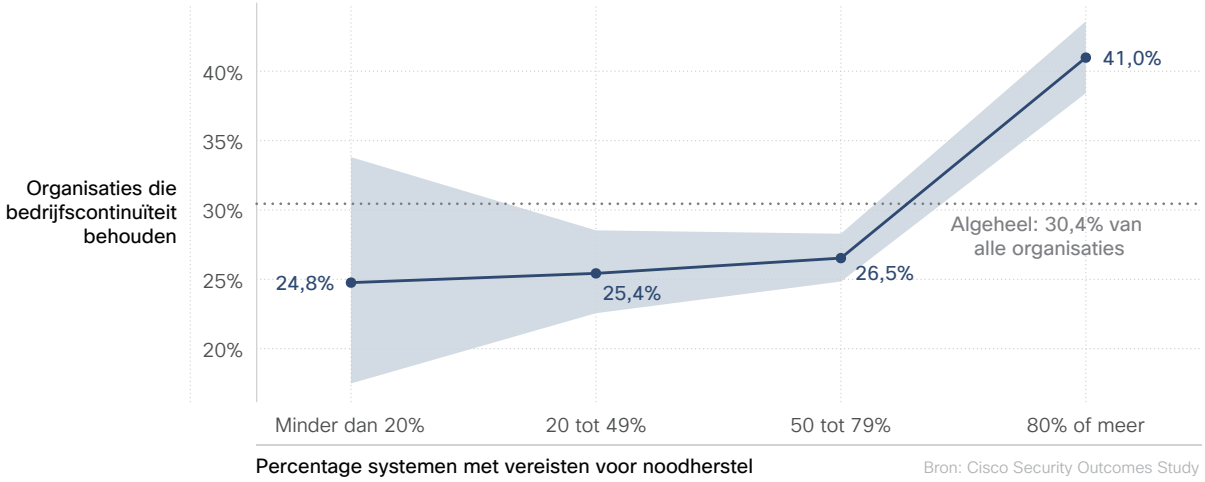
Hoe zit het met de dagelijkse activiteiten op het gebied van noodherstel?

Naast het aanduiden van de eindverantwoordelijke hebben we ook gevraagd wie verantwoordelijk is voor de meer tactische aspecten van noodherstel. **Activiteiten op het gebied van cyber security of gespecialiseerde teams die zich bezighouden met bedrijfscontinuïteit blijken de beste prestaties op te leveren.** Programma's die door IT werden uitgevoerd waren minder succesvol. Zichtbaarheid op directieniveau lijkt dus op alles een positief effect te hebben. De succespercentages waren statistisch gelijk, ongeacht wie de dagelijkse verantwoordelijkheid heeft, zolang de directie toezicht houdt.

Is de reikwijdte van noodherstel van belang?

Het zal u niet verbazen dat een noodgeval niet alleen plaatsvindt wanneer u er klaar voor bent. Dat geldt ook voor noodgevallen bij cyber security. Daarom is het verstandig om u zo goed mogelijk voor te bereiden op alle eventualiteiten. Dat is natuurlijk gemakkelijker gezegd dan gedaan.

Minder dan drie van de tien organisaties gaf aan dat hun activiteiten op het gebied van noodherstel ten minste 80% van hun cruciale systemen dekken. De helft viel in de categorie 50% tot 79%, en iets minder dan 20% gaf aan dat de dekking nog lager ligt. Op het eerste gezicht lijkt dat nog wel mee te vallen. Tenslotte hebben de meeste organisaties maatregelen genomen die de meerderheid van hun cruciale systemen dekken. Helaas wordt daarbij voorbij gegaan aan de vervelende eigenschap van noodgevallen om onverwacht plaats te vinden. Uit onze data blijkt dat dit vaker voorkomt dan we willen toegeven.



Afbeelding 21: Effect van dekking van cruciale middelen op mogelijkheden voor noodherstel

In afbeelding 21 is het resultaat van een nieuwe meting opgenomen die voor dit onderzoek is toegevoegd. Hiermee wordt het vermogen van de organisatie gemeten om bedrijfscontinuïteit te garanderen gedurende ontwrichtende gebeurtenissen. Het blijkt dat dit een van de drie resultaten is waarmee de respondenten de meeste moeite hebben. Daarom is het nog belangrijker om effectieve manieren te vinden om het succes te verhogen.

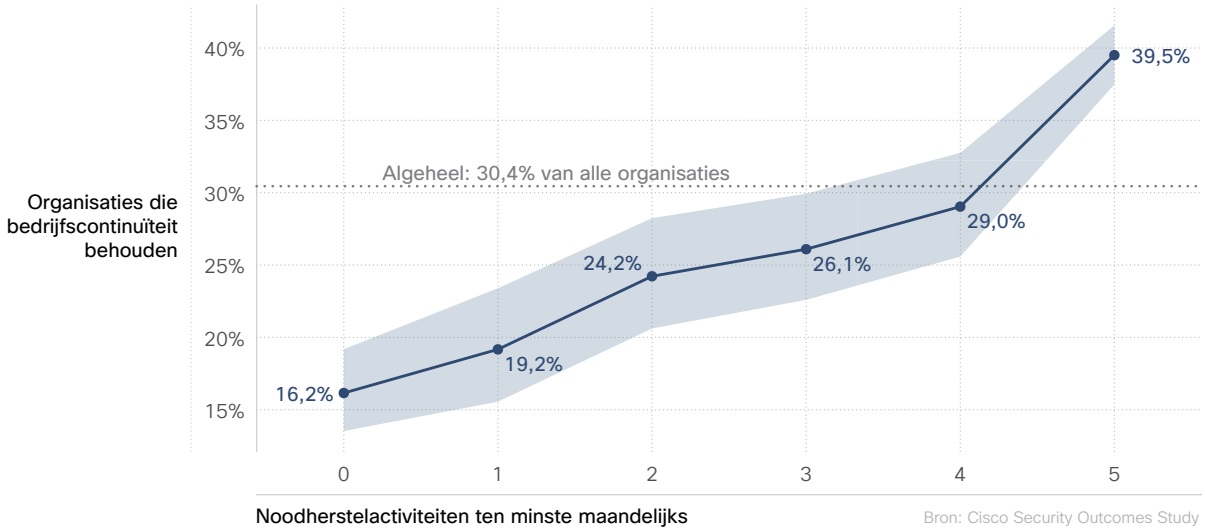
Afbeelding 21 toont belangrijk inzicht in het behoud van bedrijfscontinuïteit. **Namelijk dat er vrijwel geen sprake is van verhoging van de waarschijnlijkheid dit resultaat te behalen totdat de BCDR-processen ten minste 80% van de cruciale systemen dekken.**

Dat heeft ongetwijfeld te maken met het feit dat noodgevallen plaatsvinden wanneer we er niet klaar voor zijn. De les die we hieruit kunnen trekken, is dat we niet moeten verwachten dat investeringen in bedrijfscontinuïteit en noodherstel leiden tot directe of equivalente resultaten. Dat is geen fijn bericht, maar een noodgeval is dat nooit.

Baart oefening kunst op het gebied van noodherstel?

Dat is een goede vraag en het antwoord is duidelijk. Nee, helaas niet. Maar het is wel beter dan helemaal geen oefening. Hoeveel beter? Lees verder ...

Een bekend militair gezegde is 'Geen enkel plan overleeft het eerste contact met de vijand.' Dat geldt ook voor het cyber strijdtoneel en de BCDR-processen kunnen op veel verschillende manieren worden getest, zoals stapsgewijs doorlopen, simulatie-oefeningen, live tests, parallelle tests en volledige productietests. We vroegen de respondenten hoe vaak hun organisaties dergelijke activiteiten uitvoeren en vergeleken hun antwoord met de kans op het behouden van bedrijfscontinuïteit.



Bron: Cisco Security Outcomes Study

Afbeelding 22: Effect van tests op mogelijkheden voor noodherstel

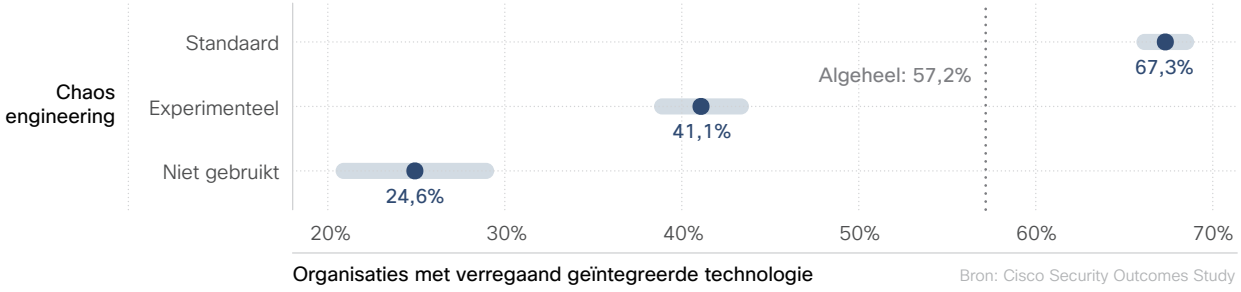
Geen van deze praktijken staken boven de andere uit waar het effectiviteit betreft, maar gezamenlijk droegen ze enigszins bij aan betere resiliency. **Organisaties die regelmatig alle vijf typen noodherstel testen, waren bijna 2,5 keer beter in staat om bedrijfscontinuïteit te behouden dan organisaties die geen enkel type testen.** De les die we hieruit kunnen trekken? Laat resiliency niet over aan het toeval. Voer regelmatig een stresstest uit van uw mogelijkheden voor bedrijfscontinuïteit en noodherstel vanuit verschillende invalshoeken.

Organisaties die regelmatig alle vijf typen noodherstel testen, zijn **2,5x** beter in staat om bedrijfscontinuïteit te behouden

Moeten we de chaos groter maken?

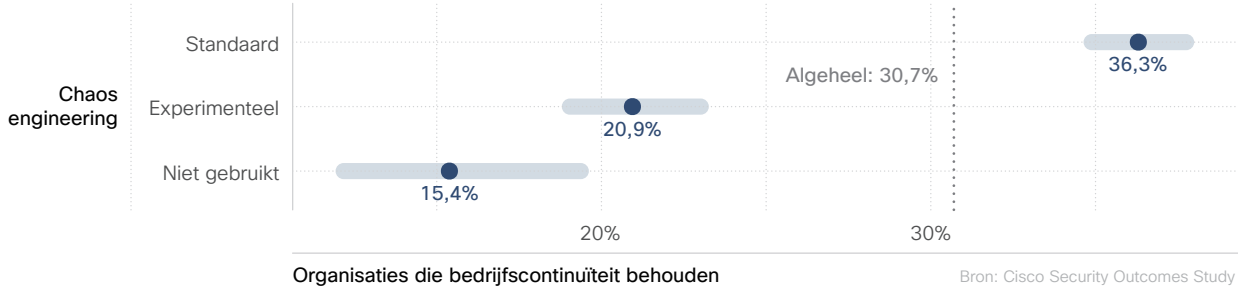
Laten we de ‘stress’ bij het uitvoeren van stresstests van uw noodherstelplan maximaliseren. We hebben het dan over chaos engineering, waarbij systemen periodiek (opzettelijk) worden verstoord om na te gaan in hoeverre ze bestand zijn tegen onverwachte omstandigheden en gebeurtenissen. Zou het steken van een spaak in het wiel (uw IT- en security systemen) uw organisatie veerkrachtiger maken? Daar gaan we nu achter komen.

We vroegen respondenten naar de mate waarin hun organisaties chaos engineering toepassen, en het bleek dat dit vaker gebeurde dan we hadden verwacht. We zagen ook een relatie tussen deze praktijk en de integratie van technologie. In afbeelding 23 kunt u zien dat twee derde van de organisaties waar chaos engineering standaard wordt toegepast verregaand geïntegreerde technologieën hebben voor herstelmogelijkheden. Of integratie nu chaos engineering vereist of mogelijk maakt is niet duidelijk. Net als bij zoveel aspecten op dit gebied is waarschijnlijk een beetje van beide van toepassing. Houd een oog open voor deze opkomende discipline, zeker als u verantwoordelijk bent voor BCDR-processen in een complexe en verregaand geïntegreerde IT-omgeving.



Afbeelding 23: Relaties tussen chaos engineering en mate van IT-integratie

Wanneer we de mate van chaos engineering vergelijken met het resultaat op het gebied van behoud van business resiliency in afbeelding 24, blijkt dat de introductie van chaos in uw netwerk aanbevelenswaardig is. **Organisaties die chaos engineering als standaardpraktijk toepassen, zijn twee keer zo vaak in staat hoge succesniveaus te realiseren dan organisaties die dat niet doen.** Als dit resultaat u verrast, bent u niet de enige. Het goede nieuws is dus dat u chaos ten goede kunt inzetten door chaos engineering toe te passen.



Afbeelding 24: Effect van chaos engineering op het behouden van business resiliency

Conclusie en aanbevelingen

We begonnen met security praktijken die in een eerder onderzoek waren aangemerkt als zeer effectief, verzamelden informatie via een nieuw onderzoek om na te gaan waardoor ze zo effectief zijn en deelden de geleerde lessen met u. We hopen dat dit rapport u praktische tips heeft gegeven om uw cyber security programma succesvoller te maken.

Maar het kan nooit kwaad om de bevindingen van een onderzoek zoals dit te overdenken en te horen wat anderen ervan vinden. We vroegen ons ervaren CISO Advisory-team zich over elk onderzocht praktijkgebied te buigen. We hebben hieronder hun belangrijkste aanbevelingen opgenomen. U kunt aanvullende inzichten en geleerde lessen vinden in onze blog-serie over de Security Outcomes Study.

Proactieve vernieuwing van technologie

"Onvoldoende investering vooraf in security vormt een groot probleem. CISO's moeten een strategie van 'kopen, aanhouden, verkopen' ontwikkelen. Ze moeten weten wat ze hebben, een aanpasbare architectuur definiëren, het risico van afhankelijkheid verkleinen en een controlelus implementeren voor toekomstige vernieuwingscycli."

Richard Archdeacon, Advisory CISO, Cisco

Goed geïntegreerde technologie

"We weten dat moderne, goed geïntegreerde IT bijdraagt aan het algehele succes van security programma's. Enkele acties die kunnen worden ondernomen om de omgeving te verbeteren: richt u op cloudgebaseerde security oplossingen, onderzoek mogelijkheden voor automation en zorg dat aankoopvereisten de mogelijkheid voor integratie van technologie omvat."

Helen Patton, Advisory CISO, Cisco @CisoHelen

Tijdige respons op incidenten

"Sterke medewerkers bieden IR-teams iets extra's. Dat is een goed startpunt, maar moet worden gecombineerd met andere elementen. Wanneer ondernemingen sterke facetten mensen, processen en technologie combineren, realiseren ze geavanceerde mogelijkheden voor bedreigingsdetectie en -respons."

Dave Lewis, Advisory CISO, Cisco @gattaca

Nauwkeurige bedreigingsdetectie

"Kies mensen met de beste vaardigheden voor uw SecOps-teams, dat is belangrijker dan het aantal medewerkers. Als u niet de mate van expertise kunt krijgen die u nodig heeft, kan automation u helpen het hiaat met uw junior medewerkers te overbruggen en is het eindresultaat net zo goed als het zou zijn met senior medewerkers."

Wendy Nather, Advisory CISO, Cisco @wendynather

Snel noodherstel

"De bevindingen in dit rapport onderstrepen de waarde van mogelijkheden voor bedrijfscontinuïteit en noodherstel, maar deze moeten wel in combinatie met andere security functies worden toegepast. Prioritering en risicobeoordeling van middelen moeten worden gedeeld met andere functies voor risicobeheer. En beheer van bedrijfsmiddelen en bedreigingsmanagement moeten nauw worden geïntegreerd om ervoor te zorgen dat alle teams volgens hetzelfde draaiboek werken."

Wolfgang Goerlich, Advisory CISO, Cisco @jwgoerlich

Over Cisco Secure

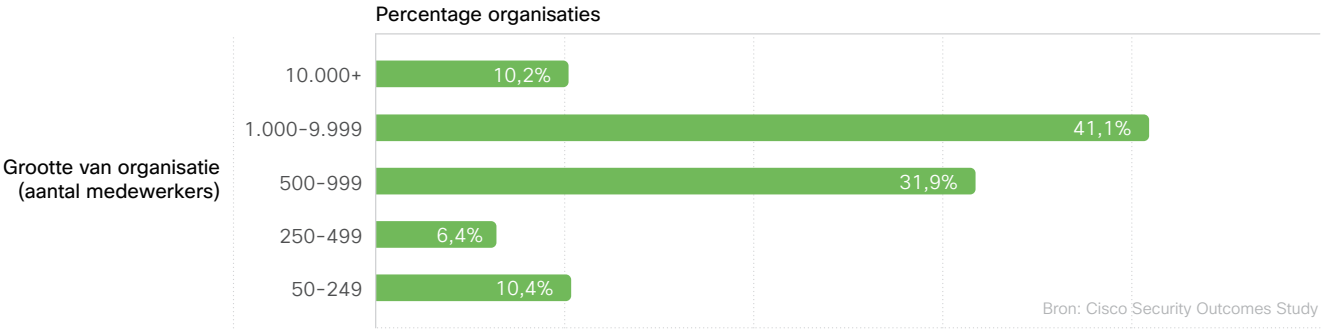
Cisco heeft zich al lange tijd bewezen als wereldwijde leider op het gebied van technologie die de kracht van het internet benut en heeft een open, geïntegreerde portfolio met cyber security oplossingen samengesteld. We zijn van mening dat security oplossingen moeten werken als een team. Ze moeten van elkaar leren. Ze moeten luisteren en reageren als één geheel. Op die manier wordt security nog systematischer en effectiever. Onze klanten hebben al jaren hun vertrouwen in ons gesteld als 's werelds grootste provider van IT-infrastructuur, netwerkservices en cyber security voor ondernemingen.

Cisco Secure gaat uit van het principe van betere security, niet meer. Cisco Secure biedt een gestroomlijnde, klantgerichte aanpak van security en zorgt dat deze eenvoudig te implementeren, beheren en gebruiken is – en dat alles samenwerkt. Mensen en onze klanten staan centraal bij wat we doen. We begrijpen dat klanten een einde willen maken aan complexiteit en ruis. Ze willen kunnen vertrouwen op hun security en hun aandacht richten op de resultaten. Dit vereist simplificatie die niet simplistisch is. Ons cloud-native platform vormt daarin een grote stap voorwaarts.

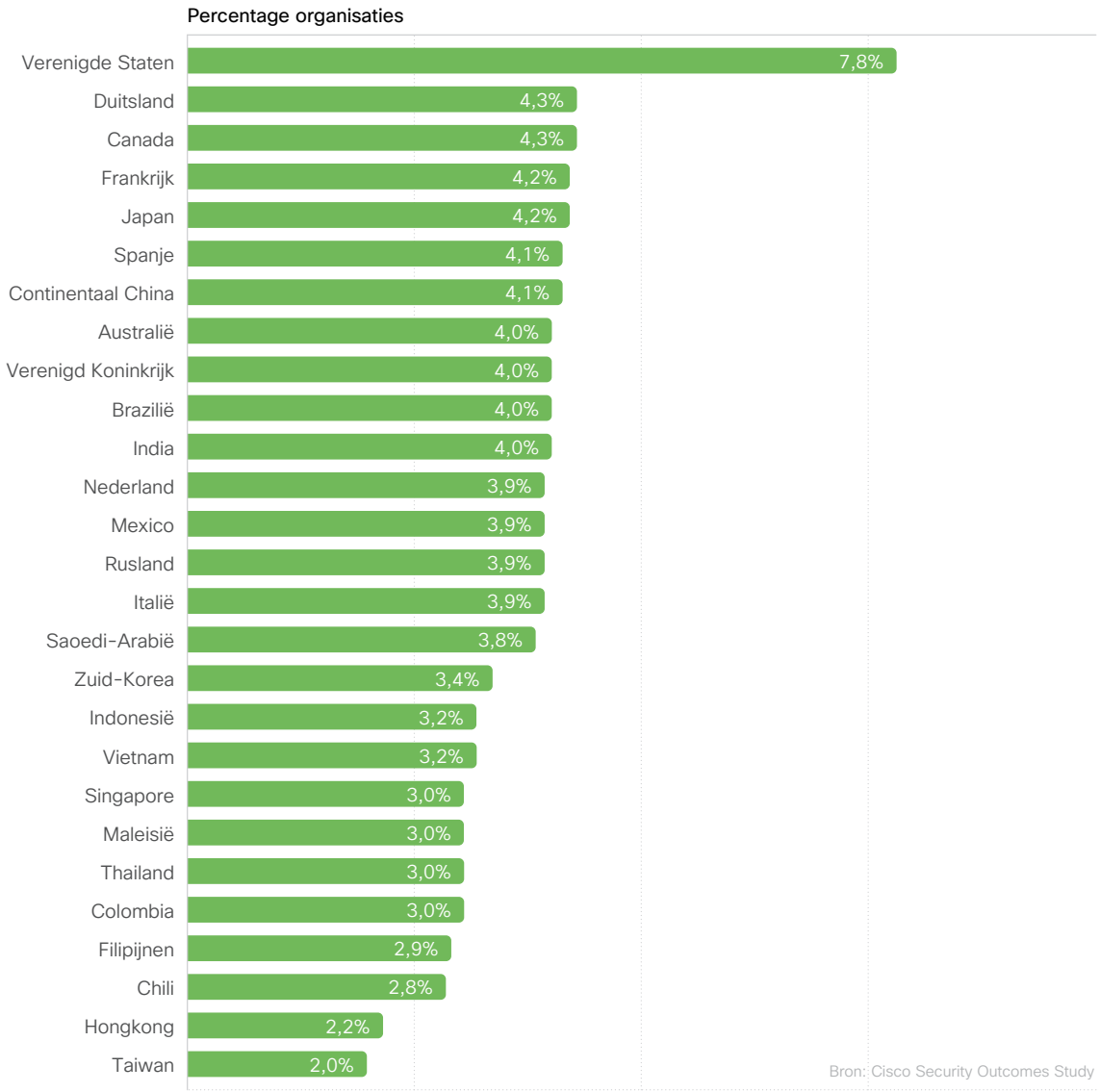
We bieden de security community de betrouwbaarheid en het vertrouwen dat ze beschermd zijn tegen bedreigingen nu en in de toekomst, met het Cisco SecureX-platform. We helpen alle Fortune 100-bedrijven overal vandaan veilig te werken met het breedste, meest geïntegreerde platform. Ga voor meer informatie over hoe we ervaringen vereenvoudigen, succes versnellen en de toekomst veiligstellen naar cisco.com/go/secure.

Bijlage: Demografische gegevens van steekproef

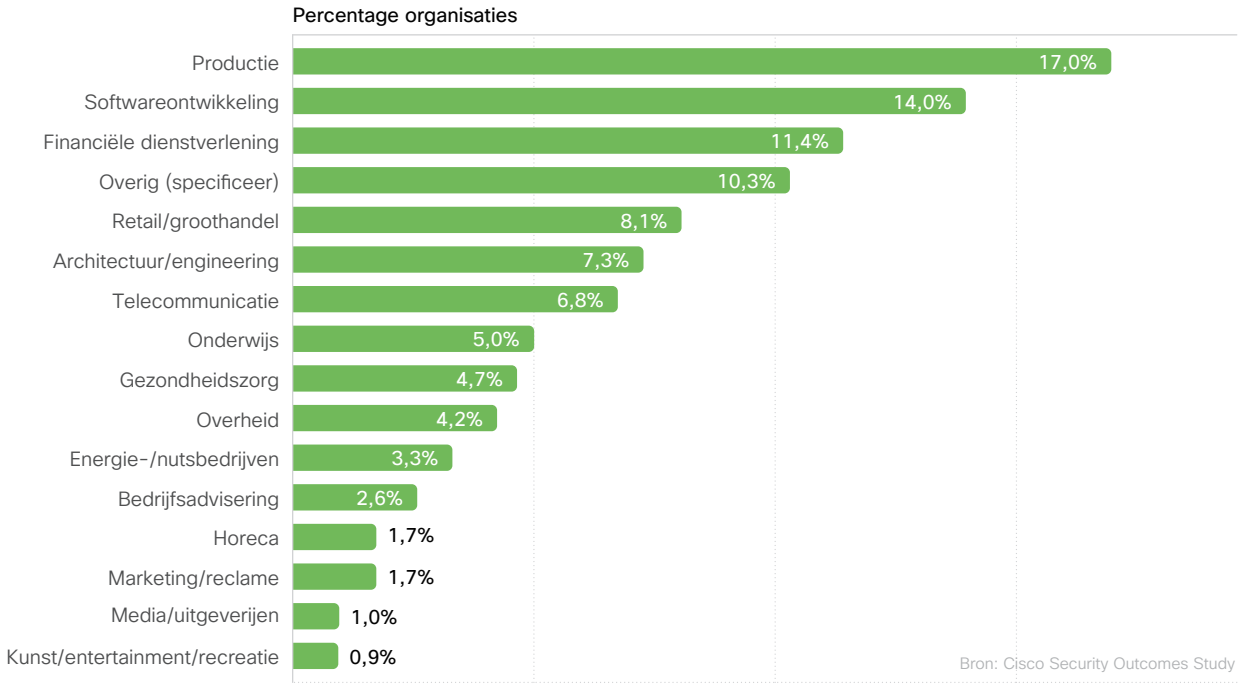
Deze bijlage bevat de demografische gegevens van de steekproef bij 5.123 gekwalificeerde responsen op dit onderzoek. We hopen dat u op basis hiervan de representativiteit van de bevindingen kunt bepalen.



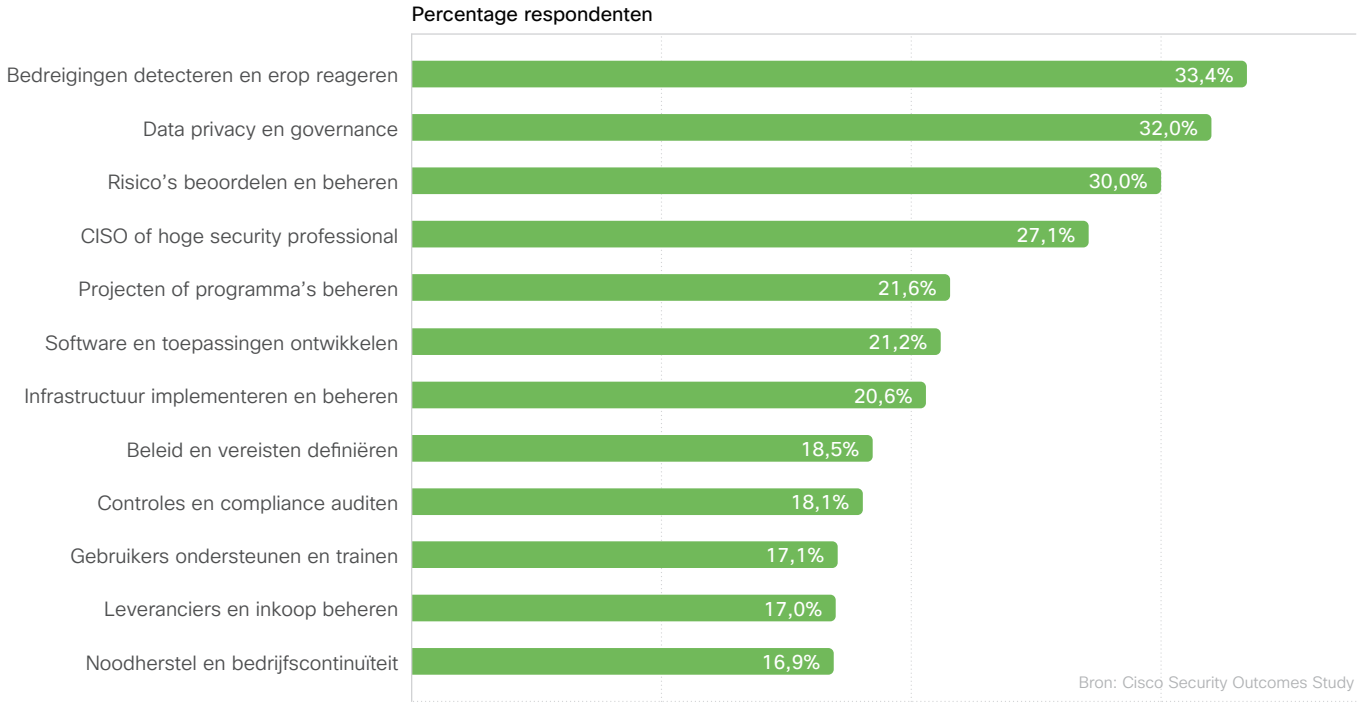
Afbeelding A1: Aantal medewerkers bij deelnemende organisaties



Afbeelding A2: Markten waarin deelnemende organisaties hun hoofdkantoor hebben



Afbeelding A3: Bedrijfstakken waarin deelnemende organisaties zijn ingedeeld



Afbeelding A4: Belangrijkste verantwoordelijkheden van respondenten

CISCO
SECURE

Hoofdkantoor Amerika
Cisco Systems, Inc.
San Jose, VS

Hoofdkantoor Zuidoost-Azië
Cisco Systems (USA), Pte. Ltd.
Singapore

Hoofdkantoor Europa
Cisco Systems International BV
Amsterdam, Nederland

Gepubliceerd december 2021

© 2021 Cisco en/of zijn dochterondernemingen. Alle rechten voorbehouden.

Cisco en het Cisco-logo zijn handelsmerken of gedeponeerde handelsmerken van Cisco en/of zijn dochterondernemingen in de VS en andere landen. Ga voor een overzicht van de handelsmerken van Cisco naar: www.cisco.com/go/trademarks. Genoemde handelsmerken van derden zijn het eigendom van hun respectieve eigenaren. Het gebruik van het woord partner impliceert geen partnerrelatie tussen Cisco en enig ander bedrijf. 779292577 | 12/21

The bridge to possible