Kiteworks

Gecertificeerd, getest, gehackt:
Waarom bug bounty-programma's de ontbrekende beveiligingslaag zijn

April 2026
Florian Scheuer – Director, Product Security, Kiteworks
Nadine Hoogerwerf – Global IT CISO, Kiteworks

Samenvatting

Echte IT-beveiliging laat zich niet certificeren en ook niet vastleggen in een rapport. Ze ontstaat daar waar een product voortdurend en onder realistische omstandigheden wordt getest op zijn weerstand — dezelfde omstandigheden waaronder aanvallers te werk gaan.

In de meeste gesprekken tussen bedrijven en hun softwareleveranciers over beveiliging blijft men ver achter bij deze ambitie. Compliancecertificeringen zijn waardevol, maar hun toetsingsobject is de organisatie, niet het product: ze tonen aan dat een bedrijf beveiligingsbewust is ingericht — niet dat zijn software bestand is tegen een gerichte aanval. Penetratietesten gaan een stap verder, maar zijn structureel begrensd: vaste tijdsvensters, vooraf bepaalde scope, één enkel team. Een pentest die op vrijdag wordt afgerond, zegt niets over de kwetsbaarheid die maandag met de volgende release in productie gaat.

Aanvallers spelen volgens andere regels. Ze zijn geduldig, hooggekwalificeerd en creatief. Geen scopedocument beperkt hen, geen rapportagedeadline drijft hen tot haast. Ze nemen de tijd om een product werkelijk te begrijpen — vaak gedurende maanden — en leggen verbanden die geen tijdgebonden test ooit had kunnen maken. Ze hebben slechts één weg naar binnen nodig, en ze hebben zoveel tijd als ze nodig hebben om die te vinden.

Bug bounty-programma’s zijn het testmodel dat aan deze realiteit recht doet. Wie zijn product openstelt voor een wereldwijd netwerk van gespecialiseerde beveiligingsexperts en valide en relevante kwetsbaarheden substantieel beloont, creëert een continue, praktijkgerichte beoordeling die geen periodieke test kan evenaren. De onderzoekers brengen diepgaande expertise mee, investeren aanzienlijke tijd en hebben een duidelijke financiële prikkel om echte kwetsbaarheden te vinden — niet om een rapport te vullen. Na verloop van tijd wordt het product op deze manier gehardend tegen potentiële aanvallen.

Voor beveiligingsverantwoordelijken is dit onderscheid direct relevant voor de besluitvorming. Compliancecertificaten en pentestrapportages blijven onderdeel van de due diligence — maar ze vormen de minimumvereiste, niet het kwaliteitskenmerk. De werkelijk bepalende vraag is een andere: investeert deze leverancier in een continue, realistische beveiligingsbeoordeling? Heeft hij een bug bounty-programma, hoe lang loopt het al, hoe breed is de scope — en zijn de beloningen hoog genoeg om de onderzoekers aan te trekken die werkelijk relevante kwetsbaarheden kunnen identificeren?

Kiteworks heeft precies deze structuur opgebouwd. Voor ons kernproduct draaien we meerdere bug bounty-programma’s — zowel private als publieke — op twee onafhankelijke platforms. Voor elk product dat via een overname deel uitmaakt van de Kiteworks-groep, starten we een eigen programma. We laten onszelf meten aan de norm die we u aanraden aan uw leveranciers te stellen — want als op enig moment niet meer de vraag is of er een certificaat aanwezig was, maar of werkelijk alles is gedaan om een beveiligingsincident te voorkomen, dan telt slechts één antwoord: een antwoord dat op alle drie de niveaus is gebouwd: governance, technische validatie en continue beveiligingsbeoordeling.

Inhoudsopgave

1. De eigenlijke vraag

Wanneer bedrijven een softwareleverancier evalueren, is de penetratietest uitgegroeid tot het standaardbewijs voor beveiliging. Leveranciers laten testen uitvoeren, ontvangen rapporten en stellen samenvattingen beschikbaar voor potentiële klanten. Vereisten worden ingevuld, checklists afgevinkt. Het geheel maakt een grondige indruk — een team van specialisten, een gedefinieerde methodiek, een schriftelijk rapport met geïdentificeerde kwetsbaarheden en aanbevelingen. De vraag die daarbij wordt gesteld, luidt: bent u getest? De vraag die er werkelijk toe doet, luidt: is uw product veilig? Dat is niet hetzelfde.

Daarbij heeft een penetratietest zeker zijn waarde. Het is een legitieme en zinvolle beveiligingsmaatregel, en bedrijven die regelmatig testen laten uitvoeren, zijn aantoonbaar beveiligingsbewuster dan bedrijven die dat nalaten. Het probleem ligt niet in de penetratietest zelf, maar in het gevaar om uitsluitend op de uitkomsten ervan te vertrouwen en de beveiliging daaraan af te meten.

Software is niet statisch, en een momentopname kan aan deze realiteit geen recht doen. De code ontwikkelt zich voortdurend, afhankelijkheden veranderen, nieuwe functionaliteit vergroot het aanvalsoppervlak en deployments brengen configuratiewijzigingen met zich mee die geen eerdere test had kunnen voorzien. Een aanvaller die vandaag het product van een leverancier in het vizier neemt, interesseert zich niet voor de scope of het tijdschema van een engagement dat maanden geleden werd afgesloten.

Wie het dreigingslandschap werkelijk een stap voor wil zijn, begrijpt dit verschil. Penetratietesten zijn een waardevolle maar beperkte bouwsteen — en wie beveiliging serieus neemt, investeert verder: in continue, op prikkels gebaseerde tests die de realiteit van daadwerkelijke aanvallen simuleren. Het belangrijkste instrument daarvoor is het bug bounty-programma.

Dit whitepaper laat zien wat penetratietesten presteren — en waar hun structurele grenzen liggen. Het pleit voor bug bounty-programma's niet als vervanging van bestaande beveiligingsmaatregelen, maar als de beslissende maatregel die de kloof overbrugt tussen een solide beveiligingskader en een werkelijk veilige en veerkrachtige operationele beveiligingsarchitectuur. En het biedt beveiligingsverantwoordelijken concrete handvatten bij de leveranciersselectie — want de juiste vragen al aan het begin stellen, is zelf een beveiligingsbeslissing.

2. Compliance en certificering: fundament, geen eindpunt

Voor bedrijven die met gevoelige gegevens werken of kritieke diensten leveren, is de implementatie van een complianceprogramma terecht essentieel. Kaders zoals ISO 27001, SOC 2 of de vereisten voortvloeiend uit NIS2 en DORA bestaan omdat de praktijk heeft aangetoond dat bedrijven zonder gestructureerd beveiligingsbeheer voorspelbare en vermijdbare fouten maken. Certificeringen tonen aan dat een leverancier het noodzakelijke fundament heeft gelegd: verantwoordelijkheden zijn helder belegd, beleidsregels gedocumenteerd, processen voor het afhandelen van beveiligingsincidenten gedefinieerd — en het bedrijf onderwerpt zich regelmatig aan een externe beoordeling.

Dit is niet vanzelfsprekend. Een leverancier zonder dit fundament vormt een risico dat technische tests alleen niet kunnen opvangen. Ontbrekende of onduidelijke governance — onbeheerde toegangsrechten, ongedocumenteerde systemen, ontbrekende noodplannen — creëert kwetsbaarheden van organisatorische aard. Compliancekaders zijn precies bedoeld om dergelijke lacunes te dichten — en ze doen dat effectief.

Toch is het van belang de grenzen van deze kaders goed te begrijpen.

Certificeringen beoordelen of een bedrijf beveiligingsbewust is ingericht en ook zo handelt. Ze toetsen processen, documentatie, organisatiestructuren en de geleefde beveiligingscultuur. Wat ze niet beoordelen — en structureel niet kunnen beoordelen — is of de concrete software die dit bedrijf ontwikkelt of beheert, uitbuitbare kwetsbaarheden bevat. Dat is simpelweg niet hun toetsingsobject.

Een bedrijf kan ISO 27001-gecertificeerd zijn en tegelijkertijd software uitleveren met een kritieke kwetsbaarheid in de authenticatie. Het kan een SOC 2-audit met goed gevolg doorlopen en ondertussen een koppeling beheren die onder bepaalde omstandigheden gevoelige gegevens blootgeeft. Het certificaat is in deze gevallen niet onjuist — het beantwoordt slechts een andere vraag dan de vraag die voor een aanvaller relevant is.

Dit is geen tekortkoming van de compliancekaders. Het is hun natuurlijke grens — en een grens die beveiligingsverantwoordelijken scherp voor ogen moeten houden. Certificeringen leggen het noodzakelijke fundament. Ze tonen aan dat een leverancier beveiliging als organisatie serieus neemt. Of zijn product bestand is tegen een gerichte aanval, is een andere vraag — en die vraagt om een ander antwoord.

3. De waarde en beperkingen van penetratietesten

Penetratietesten hebben zich in de beveiligingssector gevestigd omdat ze precies de vraag lijken te beantwoorden die compliancekaders niet kunnen beantwoorden. Terwijl een certificering de organisatie beoordeelt, richt een penetratietest zich op het product zelf. Een ervaren team probeert gericht kwetsbaarheden te identificeren en te misbruiken, documenteert zijn bevindingen en levert een rapport op met concrete aanbevelingen. Dat is praktijkgericht, technisch onderbouwd en productgericht.

De toegevoegde waarde is onmiskenbaar. Een zorgvuldig uitgevoerde penetratietest brengt kwetsbaarheden aan het licht die interne teams over het hoofd hebben gezien, toetst het gedrag van beveiligingsmaatregelen onder realistische omstandigheden en levert een gedocumenteerde basis voor een gestructureerd herstelproces. Voor veel compliancekaders is een penetratietest bovendien een formele vereiste — en de resultaten die het oplevert, voldoen op passende wijze aan die vereiste.

De grenzen van het model zijn echter structureel van aard. Ze weerspiegelen niet de kwaliteit van een bepaald bedrijf of team — ze zijn inherent aan de aanpak zelf.

De eerste beperking ontstaat door het tijdsbestek. Een typische penetratietest duurt één tot vier weken. Dat tijdvenster klinkt toereikend — totdat men bedenkt wat een ervaren beveiligingsonderzoeker moet doen voordat hij

überhaupt kan beginnen met het zoeken naar kwetsbaarheden. Het begrijpen van de productarchitectuur, het in kaart brengen van het aanvalsoppervlak, het identificeren van interfaces en gegevensstromen — dit alles vergt tijd en moet zijn afgerond voordat het eigenlijke werk begint. Bij een engagement van twee weken gaat een aanzienlijk deel van de beschikbare tijd op aan onboarding, scopeafstemming en het opstellen van het eindrapport. Het resterende tijdvenster voor diepgaand testen kan slinken tot enkele dagen. Voor een volwassen, functierijk product is dat zelden voldoende om verder te komen dan de meer voor de hand liggende kwetsbaarheden.

De tweede beperking ontstaat door de beschikbare expertise. Een penetratietest levert de kennis en het perspectief van het ingehuurde team — voor een beperkte periode. Zelfs de beste bedrijven hebben sterke punten én blinde vlekken. De onderzoeker die een subtiele kwetsbaarheid in de bedrijfslogica van een bestandsdelingsworkflow had gevonden, maakt mogelijk geen deel uit van het ingehuurde team. Binnen een vast engagement bestaat er geen mechanisme om dit te compenseren. Het team dat is ingehuurd, is het team dat test — en zijn blinde vlekken worden het ongecontroleerde risico van de opdrachtgever.

De derde beperking ontstaat door de testscope. Penetratietesten opereren binnen duidelijk afgebakende grenzen. Dat is begrijpelijk en vaak noodzakelijk — een onduidelijk gedefinieerde scope creëert operationele risico's en juridische onzekerheden. De consequentie is echter dat relevante delen van het werkelijke aanvalsoppervlak mogelijk ongetest blijven. Aanvallers interesseren zich niet voor scopedocumenten. Ze onderzoeken de koppeling die uit het engagement was uitgesloten, het legacy-eindpunt dat als niet relevant werd aangemerkt, de configuratie waaraan niemand had gedacht. Wat buiten de afgesproken scope valt, verschijnt simpelweg niet in het rapport.

De vierde beperking ontstaat door de prikkelstructuur. Penetratietestbedrijven worden voor een gedefinieerde periode ingehuurd en op basis van inzet vergoed. Er is geen financiële prikkel om meer kwetsbaarheden te vinden of dieper in een product door te dringen — het engagement eindigt wanneer de tijd om is, ongeacht wat er nog onontdekt is gebleven. Dit is geen kritiek op de professionaliteit van de testers, maar een nuchtere observatie over hoe dit model werkt. Wat wordt beloond, is de oplevering van een rapport — niet de diepgang van het onderzoek.

Alles bij elkaar betekent dit: een penetratietest levert — ongeacht hoe competent uitgevoerd — een beperkte en tijdgebonden momentopname van de beveiligingsstatus van een product. Het is een waardevolle bijdrage en een passend antwoord op bepaalde compliancevereisten. Maar het is nu eenmaal een momentopname — gemaakt door een smal tijdvenster, door een team dat het product nog aan het leren kennen is terwijl de klok al loopt — en dat het eindrapport begint te schrijven voordat de verkenning werkelijk is afgerond.

4. Hoe aanvallers te werk gaan

Om te begrijpen waarom bug bounty-programma's effectief zijn, is een korte stap terug nodig — naar de dreigingsrealiteit die ze beogen weer te geven. Niet in technisch detail, maar vanuit de fundamentele asymmetrie die elk beveiligingsvraagstuk kenmerkt.

Een aanvaller die een softwareproduct in het vizier neemt, werkt onder volstrekt andere omstandigheden dan een penetratietester. Er is geen afgesproken scope, geen tijdslimiet, geen vereiste om bevindingen in een gestructureerd rapport vast te leggen. Geen onboarding, geen kick-off. De aanvaller begint gewoon — en stopt pas wanneer het doelwit oninteressant wordt of de inspanning de mogelijke opbrengst niet langer rechtvaardigt.

Geduld is daarbij de meest onderschatte factor. Terwijl een penetratietest in weken wordt gemeten, kan een gemotiveerde aanvaller maanden besteden aan het werkelijk doorgronden van een product voordat hij een concrete aanval inzet. Hij leest documentatie, test randgevallen, observeert het gedrag van de applicatie onder ongebruikelijke omstandigheden en bouwt een steeds gedetailleerder beeld van het systeem op. De kwetsbaarheid die hij uiteindelijk misbruikt, wordt vaak pas zichtbaar na deze lange observatiefase — iets wat geen tijdgebonden engagement had kunnen blootleggen.

Specialisatie is de tweede bepalende factor. Aanvallers vormen geen homogene groep die volgens een uniform schema te werk gaat. Het betreft een divers netwerk van hooggekwalificeerde individuen — iemand die al jaren authenticatieprotocollen analyseert, een ander die zich uitsluitend bezighoudt met kwetsbaarheden in bestandsverwerking, een derde die de specifieke eigenaardigheden van een bepaald framework door en door kent.

Elk product trekt vroeg of laat de aandacht van iemand wiens expertise toevallig precies aansluit op zijn meest kwetsbare punten. Geen vast samengesteld team kan deze breedte aan specialistische kennis evenaren.

Creativiteit is de derde factor. Werkelijk ernstige kwetsbaarheden worden zelden geïdentificeerd door het afwerken van checklists. Ze ontstaan vaak uit een combinatie van zwakheden: een fout in één component die pas kritiek wordt wanneer deze wordt gecombineerd met een onvolkomenheid in een andere; een ontwerpveronderstelling die in alle bekende scenario's klopt, maar faalt bij een bepaalde reeks acties waarop niemand was gekomen. Zulke ontdekkingen vereisen niet alleen technische vaardigheid, maar ook echte nieuwsgierigheid en de bereidheid om ongebruikelijke sporen te volgen — het resultaat van diepe vertrouwdheid met een doelwit, niet van een gestructureerde methodiek onder tijdsdruk.

De conclusie voor security testing is ondubbelzinnig: wie werkelijk bedreigende kwetsbaarheden wil identificeren, heeft een testmodel nodig dat weerspiegelt hoe aanvallers daadwerkelijk te werk gaan. Geduldig, gespecialiseerd, creatief en zonder kunstmatige beperkingen. Dit model vindt in een bug bounty-programma een veel betere tegenhanger dan in een penetratietest.

5. Bug bounty-programma's: continue beveiliging in de praktijk

Een bug bounty-programma is in de kern een uitnodiging. De leverancier stelt zijn product open voor beoordeling door een wereldwijd netwerk van beveiligingsexperts en verbindt zich ertoe valide en relevante kwetsbaarheden substantieel te belonen. De hackers beslissen zelf of ze deelnemen — op basis van hun interesse, expertise en de inschatting of hun vaardigheden aansluiten bij het doelwit. Er is geen vaste einddatum, geen vooraf onderhandelde scopebeperking en geen vooraf bepaald team.

Precies dit structurele verschil met de penetratietest verklaart waarom bug bounty-programma's een fundamenteel ander effect hebben.

Continue dekking in plaats van een periodieke momentopname. Een bug bounty-programma loopt parallel aan de productontwikkeling. Nieuwe functionaliteit valt automatisch binnen de scope. Bijgewerkte afhankelijkheden kunnen direct worden onderzocht. Verandert een configuratie, dan merken ervaren hackers die het product al goed kennen wanneer iets zich anders gedraagt dan verwacht. Het assessment hoeft niet opnieuw te worden opgezet wanneer de code zich verder ontwikkelt — het loopt gewoon door en weerspiegelt de actuele staat van het product.

Toegang tot een brede kennispool in plaats van een vast team. In plaats van de vaardigheden van één ingehuurd bedrijf trekt een bug bounty-programma hackers van over de hele wereld aan met uiteenlopende specialisaties. Wie een kritieke kwetsbaarheid in een product vindt, is vaak iemand die al jaren precies de klasse kwetsbaarheden onderzoekt waarvoor deze specifieke architectuur gevoelig is. Deze match tussen specialistische kennis en een concrete kwetsbaarheid laat zich in een vast engagement niet forceren — ze ontstaat vanzelf uit de dynamiek van een open programma.

Diep productbegrip als basis voor kwalitatief hoogwaardige resultaten. Hackers binnen een bug bounty-programma zijn niet gebonden aan een tijdvenster van twee weken. Wie een programma de moeite waard vindt, kan weken of maanden investeren in het doorgronden van het product voordat de eerste kwetsbaarheid wordt gemeld. Dit geaccumuleerde begrip is de voorwaarde voor het ontdekken van complexe, geketende kwetsbaarheden — kwetsbaarheden die alleen zichtbaar worden door observaties uit verschillende delen van het product met elkaar te verbinden. Precies deze kwetsbaarheden blijven bij tijdgebonden engagements vaak onontdekt — en precies zij vormen in de praktijk het grootste risico.

Financiële prikkels borgen de kwaliteit van de resultaten — maar alleen als ze voldoende aantrekkelijk zijn. Hackers worden beloond voor valide kwetsbaarheden, niet voor bestede tijd. Er is geen reden om een rapport op te vullen met kwetsbaarheden van geringe relevantie, en geen reden om de zoektocht te staken wanneer een deadline nadert. Wie vermoedt dat er in een bepaald onderdeel van het product iets wezenlijks schuilt, zoekt door — omdat de beloning voor een kritieke kwetsbaarheid doorgaans onevenredig aantrekkelijk is. Het programma beloont resultaten, niet inspanning.

Deze dynamiek werkt echter alleen wanneer substantieel wordt beloond. Ervaren hackers hebben keuze. Ze bepalen zelf waar ze hun tijd in investeren — en kiezen programma's die hun werk passend belonen. Een programma dat slechts symbolische bedragen uitkeert, mag geen serieuze inzet verwachten. Een programma dat competitief beloont en daarmee signaleert dat de leverancier externe beoordeling werkelijk waardeert, trekt de hackers aan die werkelijk relevante kwetsbaarheden kunnen identificeren. De hoogte van de beloning is geen kostenpost om te minimaliseren — het is de bepalende hefboom voor de kwaliteit van de resultaten.

Langetermijneffect: het product wordt veiliger naarmate de tijd vordert. Dit is wellicht het meest wezenlijke voordeel voor klanten die de beveiligingsinzet van een leverancier willen beoordelen. Met elke gemelde en verholpen kwetsbaarheid neemt de weerbaarheid van het product toe. Structurele zwakheden — architectuurpatronen die steeds opnieuw kwetsbaarheden genereren, problematische afhankelijkheden, terugkerende tekortkomingen in het authenticatieontwerp — worden zichtbaar door de opeenstapeling van meldingen en kunnen fundamenteel worden aangepakt in plaats van slechts symptomatisch. Een leverancier die al meerdere jaren een serieus bug bounty-programma uitvoert, werkt met een product dat door dit proces continu is gehardend. Dat is een kwalitatief ander beveiligingsniveau dan een niveau dat wordt gehandhaafd door incidentele tests.

Voor klanten heeft dit een zeer wezenlijke betekenis: de kans om slachtoffer te worden van een beveiligingsincident dat door het eigen testproces van de leverancier had kunnen worden voorkomen, is aantoonbaar kleiner. Geen enkel beveiligingsprogramma elimineert risico's volledig — maar een goed geleid bug bounty-programma verkleint ze meetbaar. En in een dreigingslandschap waarin de vraag niet luidt of aanvallen worden geprobeerd, maar of ze slagen, is dat precies de maatstaf waaraan beveiligingsinvesteringen moeten worden afgemeten.

6. De drie niveaus van volwassen beveiliging

Wat de voorgaande paragrafen duidelijk maken, is niet dat de implementatie van een compliancekader onjuist is of penetratietesten geen waarde hebben. Het maakt slechts duidelijk dat beveiliging geen eendimensionaal concept is: voor een integrale aanpak zijn verschillende niveaus vereist — en elk van die niveaus lost een ander probleem op. Het is een fundamentele fout te veronderstellen dat men een van deze niveaus kan overslaan of ervan kan afzien.

De drie niveaus laten zich als volgt beschrijven.

Niveau 1 — Governance en processen. Dit is het fundament dat compliancekaders en certificeringen opbouwen en toetsen. Het beantwoordt de vraag: is dit bedrijf beveiligingsbewust ingericht en handelt het ook zo? Heldere verantwoordelijkheden, gedocumenteerde beleidsregels, gedefinieerde processen voor het afhandelen van beveiligingsincidenten, regelmatige trainingen, externe audits — dit zijn de bouwstenen van volwassen beveiligingsbeheer. Dit is het fundament voor al het overige. Een technisch nog zo geavanceerd beveiligingsprogramma dat op disfunctionele governance rust, zal een bedrijf niet behoeden voor de voorspelbare fouten die solide processen moeten voorkomen. Dit niveau is onmisbaar — en het is volledig terecht om van leveranciers de bijbehorende aantoonbaarheid te verlangen.

Niveau 2 — Periodieke technische validatie. Dit is het niveau waarop penetratietesten zijn gesitueerd. Het beantwoordt de vraag: heeft een gekwalificeerd team uitbuitbare kwetsbaarheden geïdentificeerd toen het dit product onder gedefinieerde omstandigheden onderzocht? Het levert technische diepgang die governancebeoordelingen niet kunnen bieden — concrete kwetsbaarheden, reële aanvalspaden, uitvoerbare aanbevelingen. Voor veel compliancekaders is het bovendien een formele vereiste, waaraan het op passende wijze voldoet. De eerder beschreven beperkingen doen geen afbreuk aan de waarde ervan — ze definiëren het toepassingsgebied. Een penetratietest is een waardevolle en noodzakelijke bijdrage, maar geen volledig beeld van de beveiligingsstatus van een product.

Niveau 3 — Continue beveiligingsbeoordeling. Dit is het niveau waarop bug bounty-programma's zijn gesitueerd — en het niveau dat de meeste bedrijven en leveranciers nog niet volledig hebben ingericht. Het beantwoordt de vraag: is dit product bestand tegen de aandacht van gekwalificeerde, gemotiveerde en hooggekwalificeerde hackers die zonder kunstmatige beperkingen werken? Het weerspiegelt de omstandigheden waaronder echte aanvallen plaatsvinden. Het loopt continu, past zich aan de productontwikkeling aan en levert resultaten die de andere twee niveaus structureel niet kunnen opleveren. Het vervangt niveau 1 en niveau 2 niet — het bouwt erop voort. Maar zonder dit niveau blijft het beveiligingsbeeld fundamenteel onvolledig.

De meeste bedrijven hebben niveau 1 ingericht. Velen hebben niveau 2 in enige vorm. Slechts weinigen hebben serieus in niveau 3 geïnvesteerd — en precies in deze lacune nestelt zich het restrisico dat uiteindelijk tot beveiligingsincidenten leidt.

De praktische consequentie is helder. Bij de beoordeling van de beveiligingsstatus van een leverancier dienen aanwijzingen voor niveau 1 en niveau 2 als minimumvereiste te gelden, niet als kwaliteitskenmerk. De bepalende vraag — de vraag die een werkelijk beveiligingsgerichte leverancier onderscheidt van een die slechts de schijn wekt — is of niveau 3 aanwezig is, hoe serieus het is ingericht en hoe lang het al loopt.

Een leverancier die deze vraag concreet en transparant kan beantwoorden, heeft een verplichting op zich genomen die verder gaat dan het slagen voor een audit — namelijk de voortdurende blootstelling van zijn product aan de toetsing waaraan het in de werkelijkheid moet voldoen.

7. Wat u van uw leverancier mag verwachten

Beveiliging is uiteindelijk ook een kwestie van de toeleveringsketen. Het eigen beleid, de geïmplementeerde maatregelen en de verworven certificeringen beschermen een bedrijf niet tegen kwetsbaarheden in de producten waarvan het afhankelijk is. Het beveiligingsniveau van uw leverancier bepaalt uw eigen beveiligingsniveau — ongeacht of het inkoopproces dat al weerspiegelt.

Dit is de praktische consequentie van al het voorgaande. Ze wijst op een concrete verandering in de manier waarop leveranciersbeveiliging moet worden beoordeeld.

Penetratietestrapportages en compliancecertificaten dienen onderdeel te blijven van de due diligence — ze bevatten waardevolle inzichten, en een leverancier die ze niet kan overleggen, voldoet niet aan de minimumvereisten. Maar wie daarbij stopt, accepteert een beveiligingsbeoordeling die precies eindigt waar de werkelijk bepalende vraag begint.

De aanvullende vragen die moeten worden gesteld — en op wiens antwoorden het werkelijk aankomt — zijn de volgende:

Heeft u een bug bounty-programma? Al het antwoord op deze vraag is veelzeggend. Een leverancier met een actief programma heeft zich publiekelijk verplicht tot voortdurende beoordeling van zijn product. Een leverancier zonder een dergelijk programma niet.

Is het programma publiek of privaat? Publieke programma's staan open voor elke gekwalificeerde hacker. Private programma's beperken de deelname tot een uitgenodigde kring. Beide hebben hun bestaansrecht — maar een publiek programma staat voor een hogere mate van openheid en vertrouwen in de kwaliteit van het eigen product.

Hoe lang loopt het programma al? Continuïteit telt. Een programma dat al meerdere jaren loopt, heeft cumulatieve beveiligingsverbeteringen gerealiseerd die een recent gestart programma nog niet heeft kunnen leveren. De looptijd is een betrouwbare indicator voor de diepte van de beoordeling waaraan het product al is onderworpen.

Wat valt binnen de scope? Een programma dat grote delen van het werkelijke aanvalsoppervlak uitsluit, biedt een zwakkere beveiligingsgarantie dan een programma met brede dekking. Begrijpen wat wel en niet binnen de scope valt, onthult waar het vertrouwen — en de terughoudendheid — van de leverancier werkelijk ligt.

Zijn de beloningen aantrekkelijk genoeg? Een programma bestaat ook op papier wanneer de beloningen te laag zijn om serieuze hackers aan te trekken. Navraag doen naar de beloningsranges — met name voor kwetsbaarheden van hoge en kritieke ernst — geeft een duidelijk signaal over hoe serieus de leverancier externe beoordeling daadwerkelijk neemt. Een programma dat slechts symbolische bedragen uitkeert, mag geen serieuze inzet verwachten.

Hoe vloeien de resultaten terug in het ontwikkelproces? De waarde van een bug bounty-programma ligt niet alleen in de gevonden kwetsbaarheden — maar in wat ermee gebeurt. Een leverancier die een duidelijk en snel traject kan beschrijven van melding via herstel naar uitrol, heeft het programma werkelijk geïntegreerd in zijn beveiligingspraktijk — en beheert het niet als marketinginstrument.

Een leverancier die deze vragen concreet en transparant kan beantwoorden, bewijst iets wat geen certificaat kan uitdrukken: dat hij zijn product afmeet aan een norm die niet door auditors wordt bepaald — maar door de realiteit waaraan zijn klanten dagelijks zijn blootgesteld.

Dat is een wezenlijk onderscheid. En in een wereld waarin beveiligingsincidenten ook blijven voorkomen bij bedrijven met volledige complianceportefeuilles, is het mogelijk de belangrijkste beveiligingsvraag die een inkoper kan stellen.

8. De beveiligingsbelofte van Kiteworks

Bij Kiteworks was de beslissing om serieus in bug bounty-programma's te investeren noch een reactie op een auditvereiste, noch op een klantvraag. Het was de consequentie van een eenvoudig inzicht: de normen die we in dit whitepaper beschrijven en die we u aanraden aan uw leveranciers te stellen, moeten eerst voor onszelf gelden.

Onze inzet gaat ver voorbij een enkel programma. Voor het kernproduct van Kiteworks draaien we meerdere bug bounty-programma's — zowel private als publieke — op twee onafhankelijke platforms. Deze structuur is bewust gekozen: private programma's maken gerichte samenwerking mogelijk met een geselecteerde kring ervaren hackers in gevoelige of complexe productonderdelen, terwijl het publieke programma het centrale aanvalsoppervlak toegankelijk maakt voor een aanzienlijk bredere deelnemerskring. Het parallelle gebruik van twee afzonderlijke platforms diversificeert de pool verder en verkleint het risico dat blinde vlekken van één platform of community onopgemerkt blijven.

Deze inzet eindigt niet bij het kernproduct. Elk product dat via een overname deel uitmaakt van de Kiteworks-groep, krijgt een eigen bug bounty-programma — dat is een norm die we consequent toepassen. Voor klanten van bedrijven die tot de Kiteworks-familie toetreden, betekent dit een onmiddellijke en tastbare verbetering van hun beveiligingsniveau: in vrijwel alle gevallen beschikten de overgenomen producten vóór de overname niet over een bug bounty-programma. Het inrichten van een dergelijk programma behoort tot de eerste beveiligingsinvesteringen die we na een overname doen. Dat is een concreet signaal voor hoe serieus Kiteworks zijn verantwoordelijkheid neemt jegens de klanten die het overneemt — en een bewijs dat een overname door Kiteworks voor die klanten een hoger beveiligingsniveau betekent, niet een lager.

De beloningsstructuur van elk programma is erop gericht de hackers aan te trekken en te behouden die werkelijk relevante kwetsbaarheden kunnen identificeren. Meldingen behandelen we niet als geïsoleerde rapporten die worden afgevinkt — maar als operationele inzichten: geïdentificeerde kwetsbaarheden sturen het herstelproces aan, de resultaten daarvan vloeien terug in de verdere architectuurontwikkeling, en het cumulatieve resultaat is een productportfolio dat continu onder realistische omstandigheden wordt getest en gehardend.

Dit kan in de snel evoluerende wereld van software nooit volledig worden uitgesloten — maar we hebben de structuren opgebouwd die het meest waarschijnlijk maken dat kwetsbaarheden worden gevonden voordat een aanvaller dat doet, en dat er snel en transparant op wordt gereageerd wanneer ze worden geïdentificeerd.

Voor onze klanten betekent dit iets concreets: producten die continu worden beoordeeld en verbeterd — afgemeten niet aan wat compliance voorschrijft, maar aan wat echte beveiliging vereist.

9. Conclusie

Het beveiligingslandschap heeft zich in het afgelopen decennium ingrijpend ontwikkeld. Compliancekaders zijn strenger geworden, penetratietesten behoren tot de standaard en het bewustzijn van cyberrisico's was in bedrijven nog nooit zo groot. Dat is een echte vooruitgang.

Toch heeft het dreigingslandschap zich parallel hieraan ontwikkeld. Aanvallers zijn geduldiger, gespecialiseerder en creatiever dan ooit — en ze maken precies gebruik van de lacunes die structureel begrensde testmodellen achterlaten. De afstand tussen wat compliance levert en wat echte beveiliging vereist, is niet kleiner geworden. Op veel vlakken is ze groter geworden.

De kernstelling van dit whitepaper is niet ingewikkeld. Governance en certificering tonen aan dat een bedrijf beveiliging serieus neemt. Penetratietesten leveren een waardevolle maar tijdelijk en inhoudelijk begrensde inventarisatie van de kwetsbaarheden van een product. Bug bounty-programma's leveren wat geen van beide kan: een continue, realistische beoordeling door een wereldwijd netwerk van gespecialiseerde hackers die de financiële prikkel hebben om te vinden wat anderen ontgaat — en de tijd om dat ook daadwerkelijk te doen.

Elk van de drie beschreven niveaus van professioneel kwetsbaarheidsbeheer heeft zijn bestaansrecht. Geen enkel niveau vervangt het andere. Maar het niveau dat het meest direct bepaalt of een bekwame aanvaller een uitbuitbare kwetsbaarheid vindt voordat de leverancier dat doet — dat is het niveau dat in de meeste gesprekken over leveranciersbeveiliging nog altijd niet wordt bereikt.

Voor beveiligingsverantwoordelijken die leveranciers evalueren, is de boodschap helder: eis de implementatie van de organisatorische basis, maar leg de lat hoger. Certificaten en penetratietestrapportages zijn het begin van een verantwoord gesprek over cyberbeveiliging — niet de afronding ervan. De leveranciers die het dreigingslandschap werkelijk een stap voor zijn, hebben aanvullende maatregelen geïmplementeerd: ze hebben hun producten opengesteld voor continue beoordeling, geïnvesteerd in de kwaliteit ervan en de interne processen opgebouwd om van de resultaten te leren en ernaar te handelen.

Als op enig moment de vraag niet meer luidt of er een certificaat aanwezig was, maar of werkelijk alles is gedaan om een beveiligingsincident te voorkomen — en die vraag zál worden gesteld — dan telt slechts of alle drie de niveaus van kwetsbaarheidsbeheer zijn ingericht. Niet alleen de niveaus die een auditor tevreden stellen. Alle drie.

Kiteworks

Copyright © 2026 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

www.kiteworks.com

April 2026