Voldoen aan het AI-cybersecuritymandaat van de ECB, van zes vereisten naar een concreet actieplan

Op 7 juli 2026 verplichtte de Europese Centrale Bank (ECB) alle significante instellingen om, de circa 110 banken onder haar directe toezicht, om uiterlijk 31 oktober een actieplan op bestuursniveau in te dienen tegen AI-versnelde cyberdreigingen. Dat plan moet zes focusgebieden dekken en dat vraagt om meer dan een momentopname. ilionx helpt je dit vertalen naar een concreet, onderbouwd plan, met continu bewijslast door de oplossingen van onze partner Horizon3.ai te gebruiken.

31 oktober 2026
Deadline voor het actieplan richting je Joint Supervisory Team (JST).

6 focusgebieden
Elk ECB-vereiste koppelen we aan een concrete aanpak.

DORA / NIS2
De aanpak sluit aan op bestaande verplichtingen.

De uitdaging

AI verkort de tijd tussen het ontdekken van een kwetsbaarheid en het misbruiken ervan van weken naar dagen en soms zelfs tot enkele uren. Veel security-programma's werken nog met handmatige, periodieke testcycli. Teams beheren daardoor lijsten met theoretische bevindingen, terwijl bewezen aanvalspaden.

De ECB vraagt organisaties niet om meer te doen, ze vraagt om bewijs; bewijs dat exploiteerbare risico's continu worden opgespoord, Zichtbaarheid alleen is niet meer genoeg. Het gaat om bewijslast waarop je met vertrouwen beslissingen kunt baseren.

De zes ECB-focusgebieden

Elke vereiste uit Annex 1 van de ECB-brief vertalen we samen met Horizon3.ai naar een aanpak die je vandaag kunt inzetten.

1. Bescherm je aanvalsoppervlak

Wat de ECB vraagt:

Breng al je IT-systemen in kaart, inclusief componenten van derden en open source. Monitor internetgerichte, cloud- en extern zichtbare systemen continu. Prioriteer herstel van kwetsbaarheden aan de rand van je netwerk.

Wat wij leveren:

Continue, autonome externe tests brengen je aanvalsoppervlakte in kaart via open-bronnenonderzoek (OSINT), zodat je sneller kunt reageren zodra een kritieke kwetsbaarheid opduikt. Dezelfde aanpak dekt ook cloud- en containeromgevingen en dekt ook interne dreigingen, iets wat de ECB expliciet benoemt.

2. Versnel kwetsbaarheden- en patchmanagement, op schaal

Wat de ECB vraagt:

Prioriteer scans, zet AI-ondersteunde tooling in, met de juiste veiligheidsmaatregelen en menselijk toezicht. Zorg dat je change management sneller, risicogestuurd patchen mogelijk maakt.

Wat wij leveren:

In plaats van te sturen op het aantal gemelde kwetsbaarheden prioriteren we op aanvalspaden die een aanvaller ook echt kan gebruiken. Na een fix verifieert een hertest met één klik of de patch het onderliggende risico daadwerkelijk heeft weggenomen, en een terugkerend testritme bewaakt dat structureel.

3. Verbeter monitoring, detectie en AI-gestuurde verdediging

Wat de ECB vraagt:

Versterk de monitoring van logs, netwerkverkeer en toegang, zodat indicatoren van een aanval en pogingen tot misbruik sneller worden opgemerkt.

Wat wij leveren:

We plaatsen digitale lokmiddelen (tripwires) precies op de hoog-risico aanvalspaden die tijdens het testen zijn blootgelegd: raakt een aanvaller er een aan, dan gaat er direct een alarm af. Vroege signalering en kant-en-klare testscenario's voor nieuwe kwetsbaarheden, ook als er nog geen patch voor bestaat, versnellen je respons. Bevindingen koppelen we aan de werkwijze van aanvallersgroepen die relevant zijn voor de financiële sector.

4. Versterk governance, budget, training en supply chain

Wat de ECB vraagt:

Zorg dat ICT-budget en -bezetting het tempo van de dreiging bijbenen. Borg verantwoording van externe ICT-leveranciers. Zet passende awareness-training in.

Wat wij leveren:

Rapportages op bestuurs- en toezichtniveau maken trends in je beveiliging en je gemiddelde hersteltijd (MTTR) inzichtelijk. De beveiliging van externe leveranciers testen we zonder dat zij software hoeven te installeren of systemen hoeven te koppelen, zodat je niet leunt op een vragenlijst die de leverancier zelf invult. Concrete impactdemonstraties onderbouwen je investeringsvoorstellen richting het bestuur.

Bewezen in de financiële sector

- Bij een tier-1 financiële instelling liet de eerste autonome interne pentest zien wat het verschil is tussen periodieke compliance-toetsing en continue, op bewijs gebaseerde weerbaarheid:
- 3 volledige aanvalspaden naar domeincompromittering en 586 niet eerder ontdekte kritieke bevindingen, gevonden binnen 14 uur.
- 7,2 miljoen bestanden bleken toegankelijk voor elke domeingebruiker.
- 117 systemen waarop admin-rechten konden worden verkregen via misbruik van gebruikersrechten.

5. Versterk defense-in-depth en moderniseer infrastructuur

Wat de ECB vraagt:

Ga ervan uit dat een aanvaller al binnen kan zijn, ook al lijkt de buitenkant veilig. Vertrouw daarom niemand automatisch, ook niet binnen je eigen netwerk (zero-trust), en verdeel het netwerk in kleine, afgeschermde zones zodat een aanvaller zich niet vrij kan bewegen (micro-segmentatie). Moderniseer of faseer verouderde systemen uit en bouw beveiliging vanaf het ontwerp in, niet achteraf.

Wat wij leveren:

We toetsen de basishygiëne van accounts en wachtwoorden in Active Directory, het fundament waar het vertrouwensmodel op leunt. Segmentatietests tonen aan of je maatregelen een aanvaller daadwerkelijk tegenhouden bij het bewegen door het netwerk, en verouderde of verkeerd geconfigureerde systemen komen aan het licht voordat een aanvaller ze vindt.

6. Verbeter operationele weerbaarheid en informatie-uitwisseling

Wat de ECB vraagt:

Zorg dat crisismanagement, respons bij incidenten en herstel aansluiten op DORA. Test tegen snelle, grootschalige aanvalsscenario's. Werk aan vertrouwde informatie-uitwisseling.

Wat wij leveren:

We simuleren veilig een complete aanval, inclusief het scenario waarin een aanvaller de controle over je centrale identiteitsvoorziening overneemt en zich door het netwerk verspreidt. Tijdens en na crisisoefeningen controleren we of herstelmaatregelen echt werken, en testresultaten worden automatisch omgezet in bruikbaar bewijs voor DORA-audits en het gesprek met je JST.

Waarom ilionx en Horizon3.ai

- ilionx is jouw IT-partner in Nederland, dichtbij en met kennis van de financiële sector. Voor autonome, continue pentesting werken we samen met Horizon3.ai, ontwikkelaar van het NodeZero-platform, dat zijn waarde wereldwijd op schaal heeft bewezen:
- 250.000+ production-safe autonome pentests uitgevoerd.
- 5.500+ wereldwijd geteste omgevingen.
- 4 van de 10 Fortune 10-bedrijven vertrouwen op NodeZero.
- Nul downtime over alle productietests tot nu toe.

Door de kracht van NodeZero te combineren met de lokale, sectorspecifieke begeleiding van ilionx bouw je aan een actieplan dat op bewijs leunt in plaats van op aannames.

Aan de slag

Wil je weten hoe jouw organisatie het ECB-actieplan onderbouwt met bewijs uit de eigen omgeving? ilionx denkt met je mee.
Plan een gesprek met een van onze experts

› ilionx.com/themas/security

ilionx Group B.V.
Van Deventerlaan 121
3528 AG Utrecht

+31 88 059 05 00
info@ilionx.com

www.ilionx.com