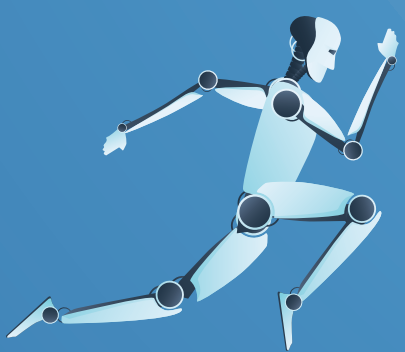
Auteur: Fook Hwa Tan is redactielid van iB-Magazine en chief quality officer bij de Northwave Group.
Hij is bereikbaar via: fookhwatan@northwave-security.com.

cybersecurity



AI in cybersecurity: navigeren in een nieuw competentielandschap

Naarmate AI dieper integreert in cybersecurity, staan professionals voor ongekende besluiten: wanneer AI-adviezen op te volgen of terzijde te schuiven? Dit artikel belicht een nieuw soort competenties die nodig zijn om deze kritieke keuzes te maken. Het focust op de vaardigheden voor het beoordelen, interpreteren en ethisch inzetten van AI, en de impact daarvan op de toekomst van cybersecurity.

De opkomst van kunstmatige intelligentie (AI) transformeert de cybersecuritywereld, waarbij nieuwe soorten competenties en besluitvormingsprocessen centraal staan. Cybersecurityprofessionals moeten nu niet alleen technische, procedurele en menselijke kennis hebben, maar ook de vaardigheden om de betrouwbaarheid en relevantie van AI-gegenereerde adviezen te beoordelen op deze vlakken. Dit vereist een nieuwe benadering van training en praktijk, waarin ethiek en kritisch denken voorop staan.

Nieuwe competenties in het AI-tijdperk

Met nieuwe competenties moet men denken aan kritisch denken en beoordelingsvermogen, ethiek en verantwoordelijkheid en AI-geletterdheid. Een cybersecurityprofessional gebruikt een AI-systeem dat netwerkverkeer analyseert om verdachte activiteiten te identificeren. Wanneer het systeem een reeks transacties als risicovol markeert, vertrouwt de professional niet blindelings op deze beoordeling. In plaats daarvan onderzoekt hij de onderliggende data, evalueert de trainingsdataset van het AI-systeem, en overweegt of de markering beïnvloed kan zijn door recente, legitieme veranderingen in netwerkgedrag of mogelijke biases in de trainingsdata.

In de context van AI en cybersecurity vereist kritisch denken dat professionals niet blindelings vertrouwen op AI-adviezen, maar deze beoordelingen analyseren en vraagtekens plaatsen bij hun geldigheid. Het gaat om het begrijpen van hoe bepaalde conclusies zijn bereikt door:

- Te beoordelen of de data die gebruikt is voor het trainen van AI-systemen relevant, actueel en vrij van biases is;
- Inzicht te krijgen in de mechanismen achter AI-beslissingen, dat helpt bij het identificeren van eventuele zwakheden of foutmarges in de algoritmes;
- Te weten dat AI-systemen bestaande vooroordelen kunnen versterken als ze worden getraind op bevooroordeelde datasets. Het is essentieel dat professionals in staat zijn om deze biases te herkennen en hier kritisch op te reageren.

Stel dat een AI-gestuurd cybersecuritysysteem een potentieel gevaarlijke softwaretoepassing op een bedrijfsnetwerk identificeert. Voordat actie wordt ondernomen, overweegt de verantwoordelijke professional de mogelijke gevolgen van het isoleren of verwijderen van deze toepassing. Zij houdt rekening met vragen zoals: 'Kan dit legitieme bedrijfsprocessen verstoren?' en: 'Is er voldoende bewijs om deze actie te rechtvaardigen?' Hierbij houdt ze niet alleen rekening met de technische, maar ook met de ethische en bedrijfsmatige implicaties, waarbij ze de privacyrechten en het welzijn van de gebruikers waarborgt.

De ethische kant van AI in cybersecurity benadrukt dat technologische vooruitgang hand in hand moet gaan met morele

overwegingen. Professionals moeten:

- Kennis hebben van fundamentele ethische principes, zoals: rechtvaardigheid, eerlijkheid en respect voor privacy hebben, dat is cruciaal;
- Beslissingen over het gebruik van AI-adviezen zorgvuldig overwegen, waarbij de verantwoordelijkheid voor de gevolgen wordt erkend;
- Voorbereid zijn op het navigeren van complexe situaties waarin verschillende ethische waarden met elkaar in conflict kunnen zijn.

Een cybersecurityteam implementeert een nieuw AI-systeem dat is ontworpen om phishing-aanvallen te detecteren. Een lid van het team neemt de tijd om de documentatie van het systeem te bestuderen, begrijpt de aard van de algoritmen die worden gebruikt en de soorten data waarop het systeem is getraind. Dit begrip stelt hem in staat om de effectiviteit van het systeem beter te evalueren en te begrijpen in welke contexten het systeem het best presteert. Wanneer het systeem een false positive geeft, kan hij door zijn kennis ingrijpen, de fout corrigeren en feedback geven voor verdere verbetering van het systeem.

In een tijdperk waarin AI een steeds grotere rol speelt, is het essentieel dat cybersecurityprofessionals niet alleen gebruikers van AI zijn, maar ook inzicht hebben in de onderliggende technologie. Dit omvat:

- Een grondig begrip van hoe AI en machine learning werken, helpt professionals om de potentie en beperkingen van deze technologieën te begrijpen;
- Inzicht in hoe AI kan worden ingezet voor diverse cybersecuritydoeleinden, zoals dreigingsdetectie en respons, verbetert de effectiviteit en efficiëntie van beveiligingsstrategieën;
- Kennis van de beperkingen van AI, zoals de afhankelijkheid van de kwaliteit van de gebruikte data en het potentieel voor onvoorziene fouten, is essentieel voor het verantwoord inzetten van deze technologie.

Door zich deze competenties eigen te maken, kunnen cybersecurityprofessionals beter geïnformeerde beslissingen nemen over het gebruik van AI, de ethische implicaties van hun acties overwegen en effectief samenwerken met AI-technologieën om de cyberveiligheid te versterken.

Besluitvorming met AI

Bij het nemen van besluiten op basis van AI of AI autonoom besluiten te laten nemen rijzen de volgende vragen: wanneer is AI te vertrouwen? Wanneer is menselijke interventie noodzakelijk? Hoe werken mens en machine samen?

AI-systemen in cybersecurity kunnen buitengewoon effectief zijn bij het uitvoeren van repetitieve en data-intensieve taken, zoals het monitoren van netwerkverkeer, het identificeren van bekende malwarehandtekeningen of het detecteren van afwijkingen die wijzen op een datalek. Het vertrouwen in AI-gebaseerde aanbevelingen hangt echter sterk af van de context en de specifieke toepassing. Bijvoorbeeld: AI kan bijzonder betrouwbaar zijn in het snel identificeren en categoriseren van bekende dreigingen, vanwege het vermogen om enorme datasets met grote snelheid nauwkeurig te kunnen analyseren; dat kunnen mensen niet.

Een goed voorbeeld is een AI-systeem dat is getraind met uitgebreide datasets van phishing-e-mails. Zodra het systeem een hoge nauwkeurigheid bereikt in het herkennen van dergelijke e-mails, kunnen cybersecurityteams op AI vertrouwen om deze dreigingen automatisch te identificeren en te isoleren, waardoor de responstijd wordt geminimaliseerd en het potentieel voor menselijke fouten wordt verkleind.

Ondanks de kracht van AI zijn er situaties waarin de nuances van menselijke ervaring en beoordeling onmisbaar zijn. Dit is met name het geval in scenario's waar de context verandert of waar AI geconfronteerd wordt met nieuwe, onbekende dreigingstypen die niet in de trainingsdata voorkwamen. Menselijke experts hebben het vermogen om bredere contextuele aanwijzingen te interpreteren, creatief te denken en beslissingen te nemen op basis van onvolledige of tegenstrijdige informatie.

Een voorbeeld is de detectie van een zero-day exploit, een nieuwe kwetsbaarheid die nog niet bekend is bij de AI. In dit geval is de expertise van een menselijke analist vereist om ongebruikelijke systeemgedragingen te interpreteren, correlaties te leggen en de dreiging te bevestigen of te ontkennen op basis van een holistisch begrip van het IT-landschap en de heersende cyberdreigingen.

Om de samenwerking tussen mens en machine effectief te maken, is een duidelijk framework voor besluitvorming essentieel. Dit framework helpt te definiëren wanneer en hoe AI-adviezen kunnen worden geïntegreerd en wanneer menselijke interventie vereist is. Een dergelijk framework zou aspecten moeten omvatten zoals:

Ondanks de kracht van AI zijn er situaties waarin de nuances van menselijke ervaring en beoordeling onmisbaar zijn

- Duidelijke criteria voor de betrouwbaarheid van AI-adviezen, inclusief prestatiebenchmarks en foutmarges;
- Protocollen voor situaties waarin AI-adviezen moeten worden geëscaleerd naar menselijke beslissers;
- Trainingsprogramma's om de AI-geletterdheid van het personeel te vergroten, zodat zij beter geïnformeerde beslissingen kunnen nemen over de AI-adviezen;
- Regelmatige evaluatie van de AI-systemen, met aanpassingen gebaseerd op feedback van menselijke gebruikers en veranderingen in het dreigingslandschap.

Een praktische uitwerking van dit framework kan worden geïllustreerd aan de hand van een incident respons protocol dat specificeert hoe alerts van het AI-systeem worden behandeld, wie verantwoordelijk is voor de eindbeoordeling, en hoe beslissingen worden gedocumenteerd en geanalyseerd voor toekomstige verbeteringen.

Deze diepgaande benadering van besluitvorming met AI in cybersecurity zorgt voor een synergie tussen menselijke expertise en machine-efficiëntie, waarbij elk zijn rol speelt in het waarborgen van de organisatorische cyberveiligheid.

Ethiek voorop

Waar mensen het meest bang voor zijn, is het feit dat machines de controle overnemen van mensen. Daarom is het belangrijk om ethiek voorop te blijven stellen. Hierbij dient aandacht aan het volgende te worden besteed: ethische overwegingen bij gebruik AI, verantwoordelijkheid voor AI-beslissingen en praktische uitwerkingen van ethiek.

Een AI-systeem dat wordt ingezet voor het screenen van veiligheidsrisico's bij werknemers moet transparant zijn over de criteria die het gebruikt, de privacy van individuen respecteren en vrij zijn van elke vorm van discriminatoire bias. De organisatie moet deze aspecten duidelijk communiceren naar alle betrokkenen en regelmatig audits uitvoeren om de naleving van deze ethische normen te waarborgen.

De implementatie van AI in cybersecurity moet gepaard gaan met strikt ethische overwegingen. Transparantie is cruciaal; gebruikers en belanghebbenden moeten begrijpen hoe AI-systemen werken, op welke data ze zijn getraind, en hoe beslissingen worden genomen. Dit bevordert vertrouwen en acceptatie.

Privacybescherming is een ander essentieel aspect. AI-systemen die persoonlijke of gevoelige informatie verwerken, moeten dit doen met respect voor de privacy van individuen, conform de geldende wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG) in de EU.

Non-discriminatie is ook een belangrijk punt: AI-systemen moeten vrij zijn van vooroordelen die kunnen leiden tot discriminatie. Dit vereist zorgvuldige selectie en monitoring van de trainingsdata om te verzekeren dat deze representatief en onbevooroordeeld is.
In het geval van een AI-gestuurde detectie van cybersecurity-dreigingen, moet duidelijk zijn wie binnen de organisatie verantwoordelijk is voor de beoordeling en actie op basis van deze detecties. Als een AI-systeem een fout maakt, zoals het ten onrechte classificeren van legitiem netwerkverkeer als kwaadaardig, moet er een procedure zijn om deze beslissing te herzien en de verantwoordelijke personen of teams moeten de bevoegdheid hebben om corrigerende maatregelen te nemen.

Organisaties moeten verantwoordelijkheidsmechanismen instellen voor beslissingen die door AI worden beïnvloed of gemaakt. Dit betekent dat er altijd een duidelijke lijn moet zijn over wie verantwoordelijk is voor de uitkomsten van deze beslissingen, inclusief de mogelijkheid om in te grijpen wanneer een beslissing herzien moet worden.

Een cybersecurityteam zou regelmatige training moeten krijgen over ethische aspecten van AI, inclusief scenario's en oefeningen die specifiek gericht zijn op de ethische dilemma's die ze kunnen tegenkomen. Ethiekcommissies of adviesraden kunnen worden ingesteld om te overleggen over complexe gevallen en richtlijnen bieden voor ethisch verantwoorde beslissingen.
Het daadwerkelijk implementeren van ethische principes in de dagelijkse cybersecuritypraktijken en besluitvormingsprocessen vereist een cultuurverandering en voortdurende aandacht voor ethische training en bewustzijn.
Door deze stappen te nemen, kunnen organisaties ervoor zorgen dat hun gebruik van AI in cybersecurity niet alleen effectief is in het beschermen tegen bedreigingen, maar ook ethisch verantwoord, transparant en in overeenstemming met de hoogste standaarden van privacy en rechtvaardigheid.

Voorbereiding op de toekomst

AI dit gezegd hebbende, hoe kunnen we ons voorbereiden op de toekomst? Hierbij moeten we denken aan educatie en training, professionalisering en dialoog om AI op een juiste manier in te zetten ter bevordering van onze doelstellingen.
In een wereld waarin AI steeds meer verweven raakt met cybersecurity, is het cruciaal dat professionals uitgerust zijn met de juiste kennis en vaardigheden. Gespecialiseerde opleidingen die de kruising van AI, ethiek en cybersecurity aanpakken, zijn essentieel. Deze opleidingen moeten niet alleen technische vaardigheden bijbrengen, maar ook diepgaand inzicht geven in de ethische implicaties van AI-gebruik in cybersecurity.

Een cybersecurityprofessional volgt een cursus waarin hij leert over de nieuwste AI-technologieën die worden gebruikt voor dreigingsdetectie. De cursus behandelt ook hoe deze systemen worden getraind, welke ethische overwegingen erbij komen kijken, en hoe bias en privacykwesties kunnen worden aangepakt. Deze kennis stelt de professional in staat om niet alleen technisch effectiever te zijn, maar ook om ethische overwegingen een plaats te geven in zijn werk.

De technologiewereld evolueert razendsnel, en wat vandaag nieuw is, kan morgen verouderd zijn. Levenslang leren en het vermogen om zich snel aan te passen aan nieuwe ontwikkelingen zijn daarom cruciale competenties voor elke professional in dit veld. Dit houdt in dat men voortdurend op de hoogte moet blijven van de laatste trends, technologieën en best practices.
Een IT-beveiligingsteam organiseert maandelijkse bijeenkomsten om de laatste ontwikkelingen op het gebied van AI en cybersecurity te bespreken. Ze nodigen regelmatig externe experts uit om lezingen te geven en nemen deel aan online forums en communities. Door deze activiteiten blijven ze niet alleen geïnformeerd, maar worden ze ook gestimuleerd om hun kennis en vaardigheden voortdurend bij te werken.

AI, ethiek en cybersecurity zijn interdisciplinaire velden die baat hebben bij een brede aanpak. De samenwerking tussen techneuten, ethici, juristen en beleidsmakers is essentieel om holistische en duurzame oplossingen te ontwikkelen. Dit soort samenwerking kan helpen bij het identificeren van gemeenschappelijke uitdagingen en het uitwisselen van beste praktijken.
Een cybersecurityorganisatie richt een werkgroep op met AI-ontwikkelaars, ethische adviseurs, juridische experts en vertegenwoordigers van regelgevende instanties. Samen beoordelen ze nieuwe AI-tools, bespreken de implicaties ervan voor privacy en beveiliging, en werken aan beleidsaanbevelingen die zowel innovatie stimuleren als ethische en juridische normen respecteren. Door deze stappen te nemen, kunnen professionals en organisaties in de cybersecuritysector, maar ook daarbuiten zich effectief voorbereiden op de toekomst, waarbij ze niet alleen technologisch vooroplopen, maar ook ethisch en maatschappelijk verantwoord handelen.

Hoe nu verder?

Terwijl AI de grenzen van mogelijkheden in cybersecurity herdefinieert, staan we op een kruispunt van uitdaging en kans. De toekomst roept professionals op om verder te kijken dan de code en circuits; het is een uitnodiging om pioniers te zijn in een tijdperk waarin technologie en menselijkheid samensmelten. In deze dynamische arena moeten we niet alleen technische meesters zijn, maar ook ethische architecten, die met inzicht en integriteit de digitale werelden vormgeven.

De reis naar morgen vraagt om een nieuwe soort moed - de moed om voortdurend te leren, uit te dagen wat we kennen, en ethische principes te verankeren in elke beslissing en innovatie. Dit is niet alleen een roep om actie, maar ook een kans om te leiden, te inspireren en de toekomst van cybersecurity actief te vormen.

Laat ons samen deze kans grijpen om niet alleen de wachters van cyberspace te zijn, maar ook de bouwers van een veilige, rechtvaardige en florerende digitale toekomst. Sta op en omarm deze uitdaging, laat zien dat wij, de cybersecurityprofessionals van vandaag, klaar zijn om de architecten te zijn van morgen. Verenigd in onze toewijding en onze vaardigheden, laten we een toekomst smeden waarin AI en ethiek hand in hand gaan, waardoor we een wereld creëren die veiliger, eerlijker en vol mogelijkheden is voor iedereen.