Cisco AI Defense: Veilig innoveren met Artificial Intelligence (AI)

De award voor Security Vendor of the Year bekroont een IT-leverancier die zich duidelijk onderscheidt in cyberbeveiliging. Met de introductie van Cisco AI Defense laat Cisco zien hoe innovatie en veiligheid samenkomen om organisaties te helpen beschermen in een tijdperk waarin AI razendsnel ontwikkelt.

Nieuwe risico's door AI

De belofte van AI brengt niet alleen kansen, maar ook complexe uitdagingen met zich mee. Uit Cisco's AI Readiness Index blijkt dat maar liefst 77% van de Nederlandse organisaties van plan is AI-agents te implementeren. Opvallend is echter dat slechts 15% aangeeft daadwerkelijk voorbereid te zijn op het beheren en beveiligen van deze AI-agents.

Tegelijkertijd moet de veiligheid van data en systemen gewaarborgd blijven. Ook volgens Gartner hebben generative AI en andere opkomende technologieën momenteel zowel positieve als negatieve invloeden op cybersecurity. AI-toepassingen maken gebruik van verschillende modellen, draaien op meerdere clouds en worden vaak gevoed met bedrijfsgevoelige data. Daarmee ontstaan risico's die traditionele beveiliging nog niet altijd kan herkennen: van hallucinaties en irrelevante uitkomsten tot promptinjecties, datalekken en ongeautoriseerd gebruik van AI-tools.

Cisco AI Defense pakt deze nieuwe realiteit aan door zich te richten op twee cruciale risico's:

1. Het veilig ontwikkelen en implementeren van AI-toepassingen;
2. Het beveiligen van de toegang tot en het gebruik van AI-toepassingen.

1. Veilig ontwikkelen en implementeren

Naarmate organisaties steeds meer AI-toepassingen bouwen en inzetten, neemt de complexiteit toe. Vaak gebeurt dit versneld, zonder uniforme beveiligingsstandaarden, waardoor kwetsbaarheden ontstaan die met bestaande securitytools niet zichtbaar zijn. AI-modellen kunnen bijvoorbeeld hallucineren en daardoor verkeerde of misleidende resultaten produceren, met directe gevolgen voor de betrouwbaarheid van besluitvorming en operationele processen. Ook zijn deze modellen gevoelig voor aanvallen, zoals promptinjecties en runtime-manipulaties, die kunnen leiden tot datalekken of de ongewenste manipulatie van uitkomsten. Het risico wordt verder vergroot door zogenoemde shadow AI: toepassingen die buiten het zicht van IT- en securityteams worden ontwikkeld of ingezet.

Met AI Defense biedt Cisco organisaties een oplossing die zich structureel richt op het aanpakken van deze risico's. De oplossing werd ontworpen om advanced testing, modelbeoordeling en runtime-security, die organisaties ondersteunen bij het identificeren van kwetsbaatheden en actuele aanvallen te mitigeren, aan te bieden. Zo doelt Cisco erop de kans op fouten, reputatieschade of compliance-issues te helpen verkleinen.

2. Toegang en gebruik beveiligen

Niet alleen de ontwikkeling, maar ook het gebruik van AI door medewerkers vormt een aanzienlijk risico. In steeds meer organisaties zetten werknemers publieke AI-tools in om bijvoorbeeld teksten samen te vatten of rapportages te genereren. Dit gebeurt vaak buiten het zicht van de IT-afdeling, waardoor er geen inzicht bestaat in welke applicaties daadwerkelijk worden gebruikt. Onbedoeld kan hierbij vertrouwelijke informatie worden gedeeld met onbeveiligde systemen, wat leidt tot datalekken of verlies van intellectueel eigendom. Bovendien ontbreekt zonder toegangsbeheer de mogelijkheid om beleidsregels af te dwingen en ongeautoriseerd gebruik te beperken.

AI Defense is erop gericht organisaties te helpen juist op dit vlak de controle te houden. De oplossing is ontwikkeld om inzicht te bieden in gebruikte AI-tools, het mogelijk te maken om regels op te stellen voor toegang tot niet-goedgekeurde toepassingen en de bescherming van bedrijfsgevoelige data tegen verlies of misbruik te ondersteunen. Op die manier kunnen organisaties de voordelen van AI benutten, terwijl kritieke informatie toch veilig zou moeten blijven.

Unieke waarde

Waar veel AI-modellen zelf slechts beperkte securityfunctionaliteit bieden, is Cisco AI Defense ontwikkeld om een overkoepelende beveiligingslaag voor uiteenlopende modellen en toepassingen te bieden. De oplossing maakt gebruik van Cisco's eigen machine learning, gecombineerd met gegevens van Splunk en Talos Threat Intelligence, zodat nieuwe dreigingen snel zouden kunnen worden opgespoord.

Daarnaast is AI Defense ingebouwd in de Cisco Security Cloud, waardoor organisaties een toekomstbestendige oplossing krijgen bedoeld om mee te groeien met hun AI-ambities én met de dreigingen die daarbij horen.

Waarom Cisco security vendor of the year is

Met AI Defense wil Cisco bedrijven in staat stellen om de kracht van AI te benutten zonder doorgaans concessies te doen aan veiligheid. Het is een innovatie die twee fundamentele risico's van AI direct aanpakt – de veilige ontwikkeling én het veilige gebruik van toepassingen – en die praktisch inzetbaar is voor zowel ontwikkelaars als securityteams. Daarmee maakt Cisco zich sterk dat het vooroploopt in het combineren van netwerken, data en beveiliging.

Cisco AI Defense is niet alleen een product, maar een belangrijke stap vooruit voor de hele IT-sector. Het is ontwikkeld om het vertrouwen van organisaties om de AI-transformatie te omarmen. Daarmee gelooft Cisco in de titel van Security Vendor of the Year.

Aanvullende info:

Website: https://www.cisco.com/site/ca/en/products/security/ai-defense/index.html

Video: https://video.cisco.com/detail/video/6368971363112