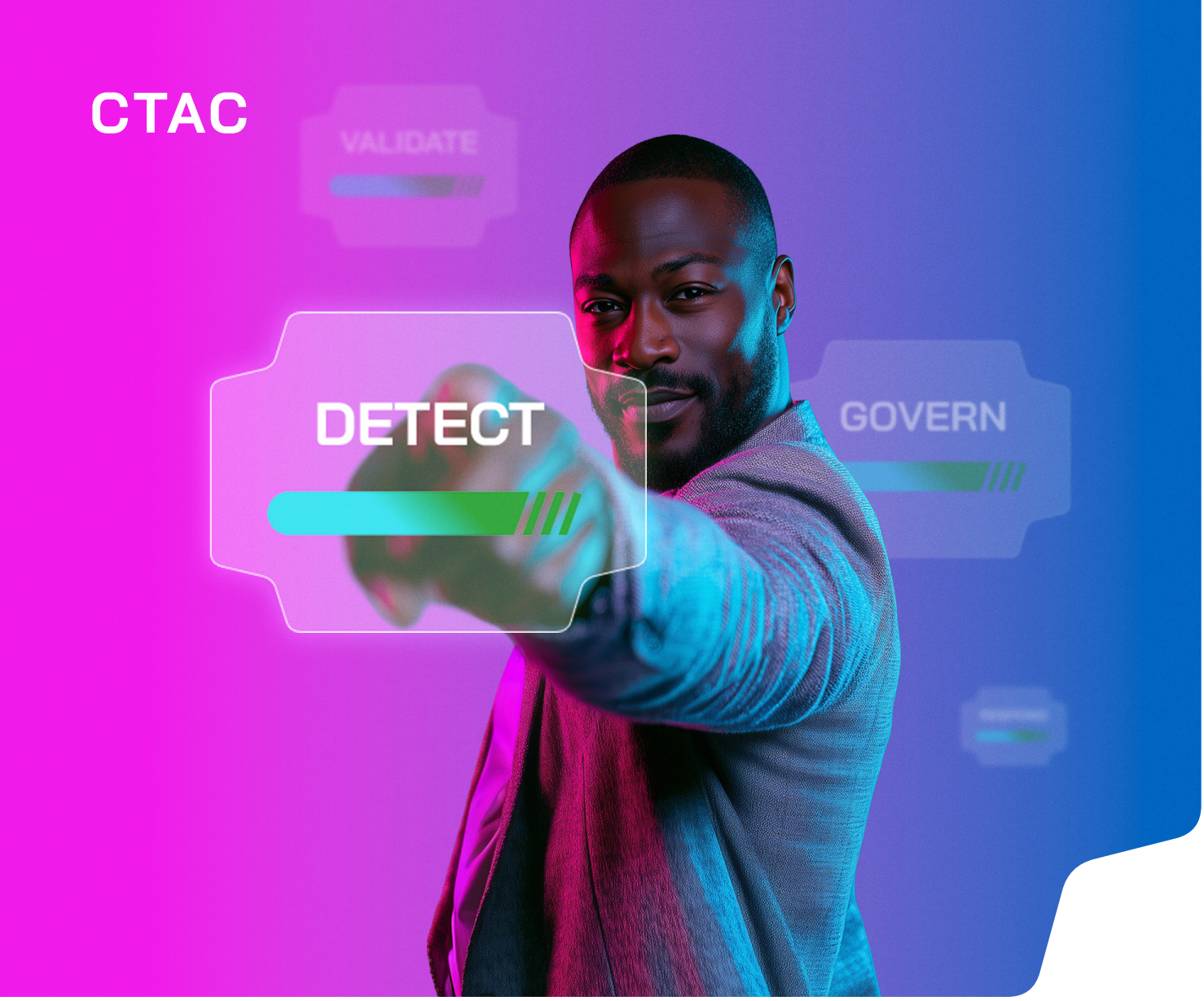
CTAC



Detect

Van zicht naar directe actie op cyberdreigingen

Cybersecurity

Cybersecurity stopt niet bij preventie. De werkelijkheid is dat aanvallen altijd een weg vinden. De vraag is niet óf je wordt aangevallen, maar of je het ziet, en op tijd handelt.

Met Detect brengen we continu in kaart wat er speelt in jouw IT-landschap. We combineren technologie, data en expertise om dreigingen direct zichtbaar te maken en in te dammen. Van endpoints tot cloud. Van gebruikers tot netwerken. Niet achteraf analyseren, maar realtime handelen. Want controle begint met zien wat er gebeurt.

MxDR (Managed Extended Detection & Response)

24/7 monitoring. Directe respons. Aantoonbare controle.

Cyberaanvallen gebeuren op ieder moment van de dag, via onbekende routes of verborgen in normaal gedrag. Ons Security Operations Center (SOC) monitort jouw volledige IT-omgeving continu. Daarbij combineren we Microsoft Sentinel, XDR-oplossingen en AI met de ervaring van gespecialiseerde security-analisten. Zo signaleren we afwijkingen vroegtijdig en grijpen we direct in. Niet pas als het misgaat, maar zodra het begint.

Wat maakt MxDR anders?

Geen losse tools of losse meldingen. Maar één geïntegreerd geheel van detectie, analyse en actie. We kijken naar het totaalbeeld: identiteiten, endpoints, netwerken, applicaties en cloudomgevingen. Daardoor herkennen we patronen die anders onopgemerkt blijven. En belangrijker: we vertalen signalen naar concrete actie.

Wat levert het op?

Je verkort de tijd tussen detectie en actie van uren naar minuten. Je beperkt de impact van incidenten door snelle containment, bijvoorbeeld door accounts of systemen direct te isoleren. Je krijgt inzicht in je securitypositie, onderbouwd met rapportages die aansluiten op compliance-eisen zoals NIS2 en ISO 27001. En je voorkomt de investering in een eigen 24/7 SOC, terwijl je wel profiteert van dezelfde kwaliteit en expertise.

Voor wie is dit relevant?

MxDR is bedoeld voor organisaties die:

- wel security op topniveau willen, maar geen eigen SOC bouwen
- werken met bedrijfskritische systemen en gevoelige data
- continu inzicht willen in hun dreigingslandschap
- moeten voldoen aan strenge compliance-eisen

MxDR (Managed Extended Detection & Response)

Wat maakt MxDR anders?

Ons SOC werkt volgens een duidelijke cyclus van detectie en actie. We monitoren continu alle relevante signalen uit jouw IT-omgeving en filteren deze direct op relevantie. Geavanceerde detectiemechanismen, gebaseerd op gedrag en intelligence, zorgen dat ook onbekende dreigingen zichtbaar worden. Zodra een incident wordt gevalideerd, starten we direct containmentmaatregelen. Denk aan het isoleren van endpoints, blokkeren van verkeer of neutraliseren van accounts.

Van detectie naar structurele verbetering

MxDR stopt niet bij het signaleren van incidenten. We zorgen dat elke detectie bijdraagt aan een sterker securityfundament. Door continu te analyseren en te optimaliseren, groeit je organisatie mee met het dreigingslandschap. Nieuwe aanvalsvormen worden sneller herkend en bestaande detectieregels worden voortdurend aangescherpt. Zo ontstaat een lerend systeem dat steeds effectiever wordt.

Altijd inzicht.
Altijd controle.

Je wilt niet alleen beveiligd zijn: je wilt het ook kunnen aantonen. Daarom leveren we periodieke rapportages met inzicht in incidenten, trends en prestaties. Daarnaast bieden we dashboards waarmee je realtime zicht hebt op wat er speelt. Relevante informatie voor zowel operationele teams als directie en auditors.

Samenwerking als sleutel tot succes

Effectieve security vraagt om heldere afspraken. Wij monitoren, analyseren en grijpen in waar nodig. Jullie voeren herstelmaatregelen door en blijven eigenaar van de omgeving. Door deze samenwerking ontstaat snelheid en duidelijkheid op de momenten dat het ertoe doet.

Snelle implementatie, direct waarde

Binnen enkele weken is MxDR volledig ingericht. We starten met een intake en bepalen samen de scope. Daarna sluiten we systemen en databronnen aan, richten detectie in en voeren een testfase uit. Pas als alles klopt, schakelen we over naar volledige 24/7 monitoring.

Shadow AI

Zicht op AI-gebruik binnen je organisatie

AI wordt steeds vaker gebruikt in dagelijkse werkzaamheden. Vaak zonder dat organisaties precies weten waar, hoe en met welke data. Dit brengt risico's met zich mee. Met Shadow AI maken we zichtbaar waar ongeautoriseerd AI-gebruik plaatsvindt en welke impact dit heeft op security en compliance.

Van detectie naar beleid

Shadow AI gaat verder dan alleen signaleren. We helpen je bij het opstellen van beleid, het inrichten van controles en het realiseren van bewustwording binnen de organisatie. Zo ontstaat een balans tussen innovatie en beheersing.

Waarom is dit nodig?

Medewerkers gebruiken steeds vaker tools zoals chatbots en code-assistenten. Vaak zonder inzicht in wat er met data gebeurt. Gevoelige informatie kan onbewust gedeeld worden met externe AI-systemen. Met risico's voor privacy, intellectueel eigendom en compliance. Shadow AI brengt deze blinde vlek in beeld.

Wat levert het op?

Je krijgt inzicht in waar en hoe AI wordt gebruikt binnen je organisatie. Je voorkomt dat gevoelige data ongecontroleerd wordt gedeeld. En je kunt gericht beleid ontwikkelen en afdwingen rond verantwoord AI-gebruik. Niet door alles te blokkeren, maar door gecontroleerd en bewust gebruik mogelijk te maken.

Cyber Threat Intelligence (CTI)

Weten wat er aankomt

Veel organisaties reageren op dreigingen. Met CTI ga je een stap verder: je anticipeert. Wij verzamelen en analyseren dreigingsinformatie uit betrouwbare bronnen en vertalen deze naar jouw specifieke situatie.

Wat betekent dat in de praktijk?

Je weet welke dreigingen relevant zijn voor jouw sector en infrastructuur. Je kunt prioriteiten stellen op basis van actuele risico's. En je verbetert de effectiviteit van je monitoring en detectie door intelligence direct toe te passen.

Het resultaat

Je beweegt van reactief naar proactief securitymanagement. En je kunt onderbouwd laten zien dat je risicogestuurd werkt.

Wat betekent dat in de praktijk?

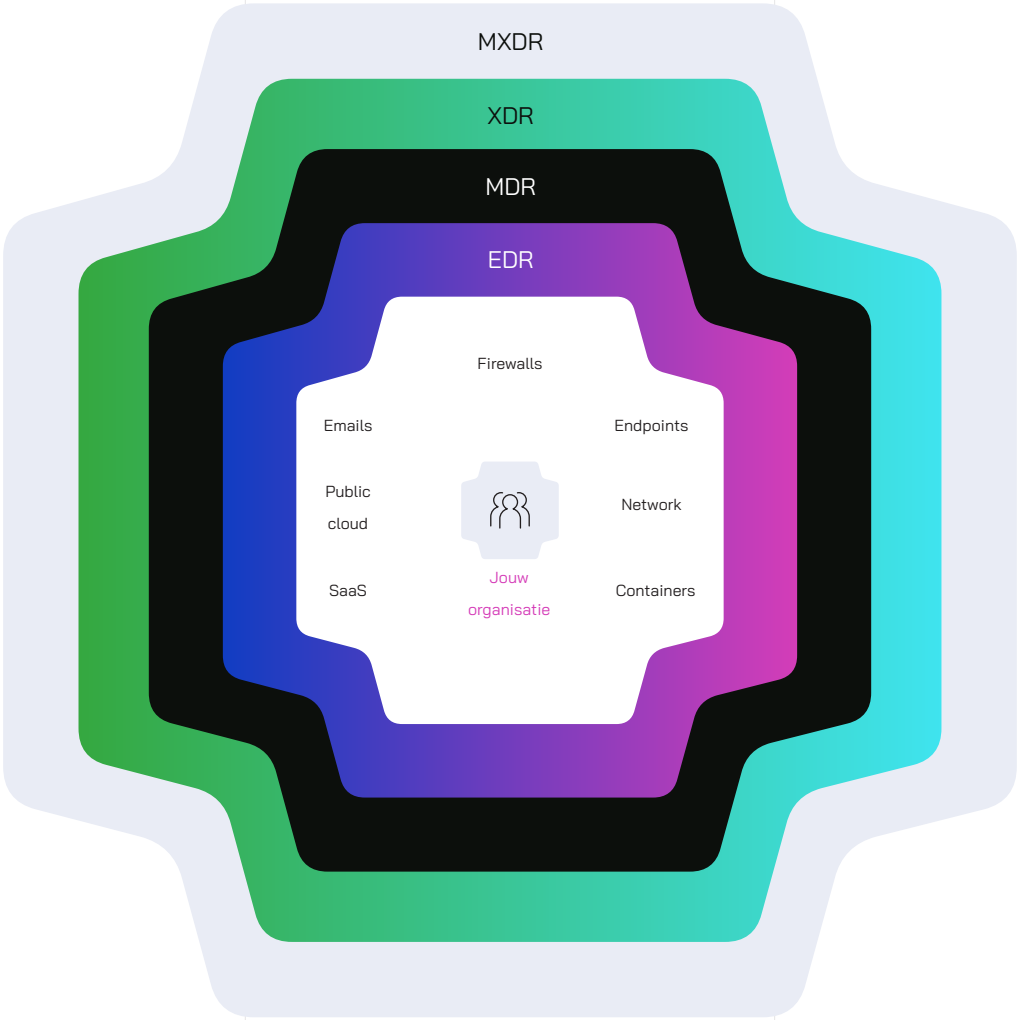
Je weet welke dreigingen relevant zijn voor jouw sector en infrastructuur. Je kunt prioriteiten stellen op basis van actuele risico's. En je verbetert de effectiviteit van je monitoring en detectie door intelligence direct toe te passen.

Eén geïntegreerde aanpak

Detect staat niet op zichzelf. MxDR, Shadow AI en CTI versterken elkaar. Samen vormen ze één geïntegreerd geheel waarin signalen, context en actie samenkomen.

Zo krijg je:

- controle over nieuwe risico's zoals AI-gebruik
- en de intelligence om vooruit te kijken
- realtime inzicht in dreigingen

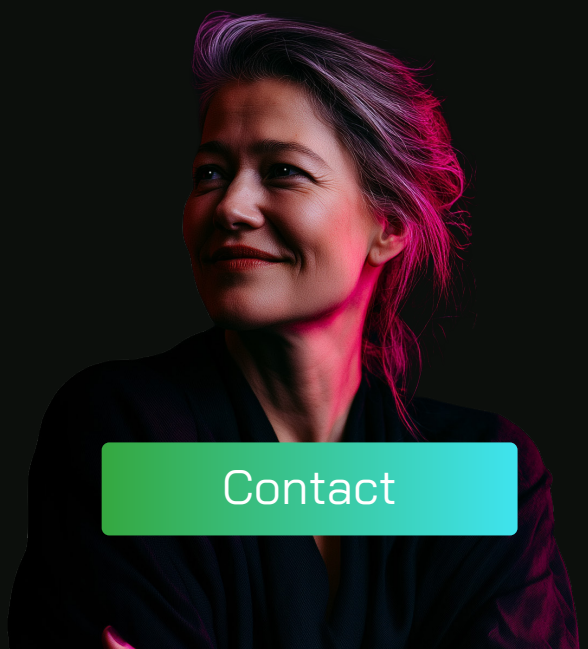


Business driven security.

Begrijpen.
Detecteren.
Direct ingrijpen.

Grip op cybersecurity begint met de juiste detectie

Of je nu aan het begin staat van je securityreis of je cybersecurity verder wilt professionaliseren: Ctac helpt je om de juiste keuzes te maken, risico's te beheersen en aantoonbaar in control te zijn.



Contact