CTAC

Respond

Direct handelen als het ertoe doet

Cybersecurity

Een cyberincident komt nooit gelegen. Maar op het moment dat het gebeurt, telt elke seconde. Hoe sneller je handelt, hoe kleiner de impact. Hoe beter je voorbereid bent, hoe meer controle je houdt.

Binnen Respond zorgen we dat je organisatie niet alleen reageert, maar ook regie houdt. Van directe inzet bij incidenten tot crisismanagement en voorbereiding. Zodat je niet hoeft te improviseren, maar weet wat te doen. Want het verschil maak je op het moment zelf.

Incident Response Retainer

Directe inzet bij incidenten: zonder vertraging

Bij een cyberincident wil je geen tijd verliezen aan zoeken naar hulp. Met de Incident Response Retainer heb je direct toegang tot een gespecialiseerd team dat klaarstaat om in te grijpen. 24 uur per dag. 7 dagen per week. Eén telefoontje is genoeg om de respons te starten.

Wat betekent dat concreet?

Zodra er een incident plaatsvindt, schakelen wij direct. We analyseren de situatie, starten forensisch onderzoek en nemen samen met jouw team maatregelen om de aanval in te dammen. Denk aan het isoleren van systemen, blokkeren van accounts of het stoppen van data-exfiltratie. Alles gericht op één doel: schade beperken.

Waarom een retainer?

Zonder voorbereiding verlies je kostbare tijd. Onder druk beslissingen nemen, leveranciers zoeken en contracten regelen, dat wil je voorkomen. Met een retainer staan alle afspraken al klaar. Inclusief prioriteit bij gelijktijdige incidenten. Daardoor kun je direct handelen.

Van incident naar inzicht

Een incident stopt niet bij containment. We analyseren wat er is gebeurd, hoe het heeft kunnen gebeuren en welke maatregelen nodig zijn om herhaling te voorkomen. Zo wordt elk incident een bron van verbetering.

Wat levert het op?

Je verkort de responstijd drastisch en beperkt de impact van incidenten. Je profiteert van een team dat jouw omgeving al kent, waardoor sneller en effectiever wordt gehandeld. En je kunt aantoonbaar laten zien dat je voorbereid bent op crisissituaties — belangrijk voor board, auditors en verzekeraars.

Crisis Management

Regie houden in een crisis

Een cyberincident is zelden alleen technisch. Het raakt je organisatie, je klanten en je reputatie. Beslissingen moeten snel genomen worden. Communicatie moet kloppen. Stakeholders verwachten duidelijkheid. Daar komt crisismanagement om de hoek kijken.

Wat doen wij?

We ondersteunen het management tijdens de crisis. We helpen bij het maken van de juiste keuzes, het organiseren van communicatie en het afstemmen met interne en externe stakeholders. Van directie tot toezichthouder. Van medewerker tot klant.

Waarom is dit belangrijk?

Zonder regie ontstaat chaos. Besluiten worden vertraagd, communicatie wordt inconsistent en de impact neemt toe. Met de juiste begeleiding blijft de organisatie controle houden, ook onder druk.

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

- Snellere besluitvorming
- betere communicatie
- een organisatie die ook in crisis professioneel blijft functioneren.

CSIRT-plan

Weten wie wat doet: vóórdat het misgaat

Op het moment van een incident wil je niet nadenken over rollen en verantwoordelijkheden. Die moeten vooraf duidelijk zijn. Met een CSIRT-plan leg je vast hoe jouw organisatie reageert op incidenten. Wie de leiding neemt, wie communiceert en welke stappen worden gezet.

Wat levert het op?

Je voorkomt ad-hoc handelen en versnelt de respons. Iedereen weet wat er verwacht wordt en hoe er gehandeld moet worden. Dat zorgt voor rust, duidelijkheid en snelheid op het moment dat het nodig is.

Meer dan een document

Een CSIRT-plan is geen papieren exercitie. Het is een praktisch draaiboek dat aansluit op jouw organisatie, processen en risico's. En een belangrijk fundament voor compliance en governance.

Oefenen & Simuleren

Voorbereid zijn door te trainen

Een plan is pas echt waardevol wanneer het in de praktijk werkt, en juist daarom trainen we met realistische scenario's die zo dicht mogelijk bij de dagelijkse werkelijkheid liggen, variërend van boardroom-simulaties tot technische aanvalsscenario's, zodat iedereen binnen de organisatie begrijpt wat er van hem of haar verwacht wordt nog voordat een echte situatie zich voordoet.

Hoe werkt dat?

We simuleren een cyberincident en begeleiden jouw teams stap voor stap door het scenario, waarbij het management leert hoe beslissingen onder druk tot stand komen en hoe communicatie effectief wordt ingericht, terwijl IT-teams tegelijkertijd oefenen met detectie en respons, waardoor tijdens de oefening direct zichtbaar wordt waar processen goed werken en waar bijsturing nodig is.

Wat levert het op?

Je krijgt inzicht in waar processen in de praktijk anders verlopen dan vooraf gedacht, terwijl je tegelijkertijd de slagkracht van je teams vergroot en de responstijd bij echte incidenten verkort, en misschien nog belangrijker: je voorkomt dat fouten en onduidelijkheden pas aan het licht komen op het moment dat de impact het grootst is.

Van reageren naar beheersen

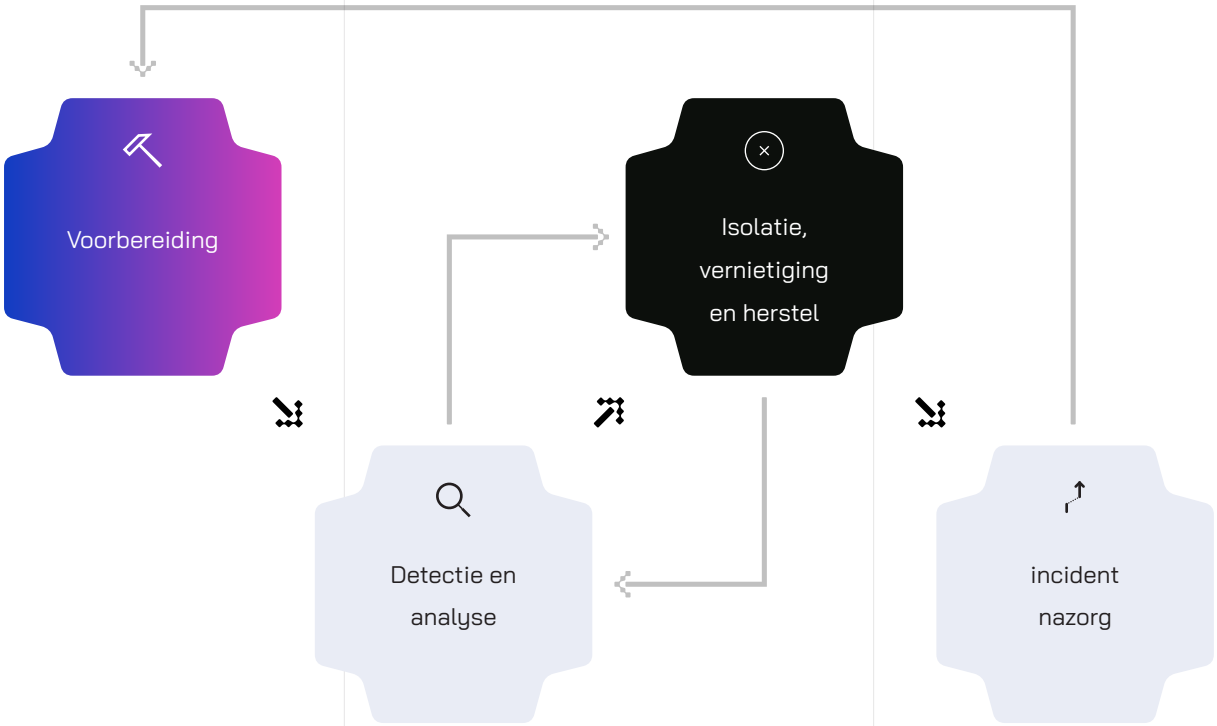
Respond gaat verder dan het afhandelen van incidenten alleen, omdat het draait om voorbereid zijn, regie houden en continu verbeteren, waarbij de combinatie van Incident Response, Crisis Management, CSIRT-planning en oefenen zorgt voor een geïntegreerde aanpak waarmee je organisatie niet alleen weet wat te doen als het misgaat, maar dit ook al in de praktijk heeft doorlopen.

Altijd voorbereid

Cyberincidenten zijn onvermijdelijk, maar onbeheersbaarheid is dat niet, en met Respond van Ctac zorg je dat je organisatie in staat is om direct te handelen bij incidenten, regie te houden tijdens crises, voorbereid te zijn met duidelijke processen en tegelijkertijd continu te blijven leren en verbeteren, zodat er geen ruimte is voor paniek of improvisatie, maar juist voor controle, snelheid en duidelijkheid.

incident repons proces

Een gids in het managen van cybersecurity bedreigingen

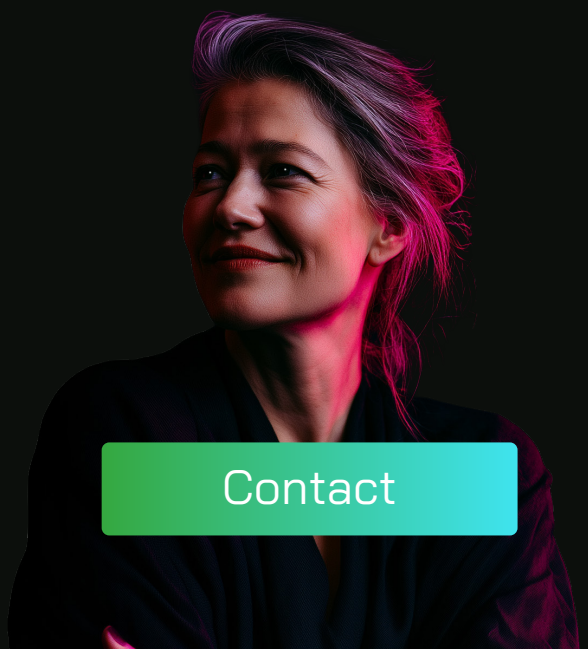


Business driven security.

Gereageerd.
Gecontroleerd.
Hersteld.

Grip op cybersecurity begint met de juiste response

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