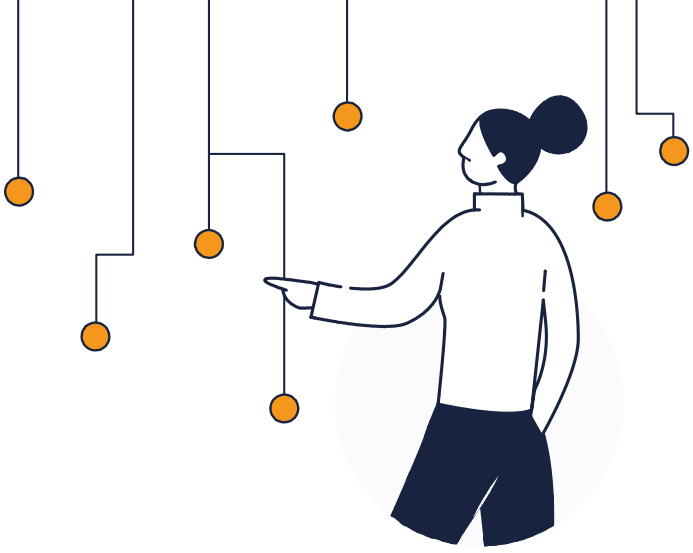

Incident Response

Reageer snel en effectief op cyberincidenten met Eye Security

Je bent net aangevallen. Wat doe je?

Het zelf oppakken? 1

Isolatie en insluiten zijn gespecialiseerde cybersecurityvaardigheden. Deze goed leren beheersen kost tijd, die je niet hebt als er een aanval plaatsvindt.

Misschien heb je een Incident Response-plan? 2

Dekt dat plan alle soorten dreigingen en gevolgen? Je hebt met elk scenario ervaring nodig om effectief met een aanval om te gaan.

Vertrouwen op je cybersecurity-software? 3

Als er eenmaal een aanval plaatsvindt, kan de software maar zoveel doen. Het is dan eigenlijk al te laat en je krijgt niet de ondersteuning die je nodig hebt.

Externe experts inschakelen? 4

Met externe experts in gesprek gaan kan lastig zijn zonder gespecialiseerde kennis en kan een hoop tijd kosten. Bovendien: lost dat langlopende kwetsbaarheden op?

Niemand wil slachtoffer van een cyberaanval worden, maar pas als je dat wel bent geweest realiseer je je hoeveel expertise er nodig is om direct controle over de situatie te krijgen. Moderne aanvallen zijn erg geavanceerd en vaardige aanvallers maken het steeds moeilijker voor bedrijven om zichzelf te beschermen en om te herstellen van een cyberaanval. Als het gebeurt, is het cruciaal om snel en effectief te reageren, om de schade en hoge kosten te beperken.

1/5
De kans op een cyberaanval

4 min
De gemiddelde reactietijd op een incident

Jouw oplossing:

Als je aangevallen wordt, wil je met de beste samenwerken – een team van experts, dat jaren ervaring heeft opgedaan in onder meer de nationale inlichtingendiensten en bij beveiligingsbedrijven. Deze mensen staan 24/7 klaar, om jou ervan te verzekeren dat je operationele processen snel weer online zijn en draaien. Een aantal incidenten die we regelmatig tegenkomen, zijn:

- Versleutelde bestanden als gevolg van een ransomware aanval
- Onverklaarbaar gedrag in operationele systemen
- Frauduleuze e-mails die door een aanvaller verstuurd zijn

We hebben alle soorten aanvallen gezien en bij alle aanvallen is het onze opdracht om het probleem snel op te lossen en om er voor jou te zijn als een lid van een uitgebreid team. Wij kalmeren en ondersteunen.

De voordelen van Incident Response

Snelle reactie
Wanneer je contact opneemt met onze incident response-hotline, starten we de analyse en nemen we direct stappen om de dreiging te beperken.

Beperkte schade
Door onze expertise snel in te zetten via Managed Detection & Response-software kunnen we jouw systemen beveiligen om verdere schade te voorkomen.

Snel weer aan het werk
Met zo'n ervaren Incident Response-team kunnen we jou ervan verzekeren dat je snel weer terug naar normaal gaat, zodat er zo min mogelijk verstoringen voor het bedrijf zijn.

Hoe Incident Response werkt

Triage
Snel het type incident identificeren en bepalen welke impact het heeft op de beschikbaarheid, privacy en integriteit van jouw data.

Kick-off
Er volgt direct een bijeenkomst om het Incident Response-proces te schetsen, zodat er een duidelijk begrip wordt gewaarborgd en er verantwoordelijkheden worden toegewezen aan alle betrokken partijen.

Insluiting
Het analyseren, insluiten en minimaliseren van de nadelige gevolgen van het incident. Er volgen nauwgezette acties om jouw digitale bezittingen te beveiligen.

Herstel
De dreiging wordt verwijderd en de systemen worden met een methodische aanpak hersteld om jouw operationele processen weer online te brengen.

Evaluatie
We nemen actie op basis van de drie waardevolle lessen uit het incident: versterk de netwerkbeveiliging, verbeter het Business Continuity Plan (BCP) en optimaliseer de reactie.

Ontmoet het team

Waarom klanten hun cybersecurity aan ons team toevertrouwen

Onze teamleden hebben een schat aan ervaring opgedaan bij de inlichtingendiensten en security-omgevingen op hoog niveau. Met ervaring in het navigeren van complexe dreigingen, bestrijden we cyberuitdagingen op een intelligente en rustige manier, waarbij we dreigingen, bestrijden we cyberuitdagingen op een intelligente en rustige manier, waarbij we voortbouwen op inzichten uit praktijkscenario's.

Vaisha

Principal cybersecurityspecialist

13+ jaar aan ervaring in IT-beveiliging

Lodi Hensen

VP Security Operations

15 jaar ervaring in cybersecurity (forensics & incident response)

Michael de Klein

Senior cyber security specialist & Teamlead MDR

5+ jaar ervaring (aanvallend en defensief)

Niels Teusink

Principal cybersecurityspecialist

17 jaar aan fulltime ervaring in IT-beveiliging

Bas van den Berg

Principal cybersecurityspecialist

8+ jaar ervaring in IT-beveiliging

Davy

Senior cybersecurityspecialist

6+ jaar ervaring in IT

Ons Incident Response-proces:

Jouw Incident Response checklist:

1 Identificatie

- Herken en bevestig snel dat er een security-incident plaatsvindt
- Definieer de omvang van het incident en het soort incident

2 Insluiting

- Isoleer getroffen systemen of netwerken om verdere schade te voorkomen
- Implementeer tijdelijke maatregelen om de impact te beperken

3 Uitroeiing

- Identificeer en elimineer de oorzaak van het incident
- Verwijder malware, dicht kwetsbaarheden en pak zwakke plekken aan

4 Herstel

- Herstel getroffen systemen zodat ze weer normaal draaien
- Valideer dat de omgeving veilig is en er geen overblijfselen van het incident meer aanwezig zijn

5 Communicatie en documentatie

- Stel relevante partijen op de hoogte, zoals het management, IT-teams en, als dat nodig blijkt, de politie
- Documenteer het incident, welke acties genomen zijn en welke lessen geleerd zijn voor toekomstige verbeteringen