DIGITALE OPSPORING

VOORKOMEN & BESTRIJDEN

DIGITAAL ONDERZOEK

CYBER SECURITY

OPLEIDINGEN

Digitale Opsporing BV | Nijverheidsstraat 8 | 5961 PJ Horst | 085-489 12 50 | www.DigitaleOpsporing.nl

DIGITAAL ONDERZOEK

KENNIS EN KUNDE

Digitale Opsporing (DO) is uniek vanwege haar expertise op het gebied van digitaal recherche onderzoek. Ons team bestaat uit gecertificeerde forensische professionals en (digitale) rechercheurs afkomstig van politie Nederland.

Door de ruime recherche ervaring van onze medewerkers en de diversiteit aan specialismen zijn wij in staat om (politie)dossiers van strafzaken en civiele procedures diepgaand te onderzoeken en te beoordelen.

U bent bij ons ook aan het juiste adres voor onderzoek naar verduistering, falsificaties, financiële fraude, internetfraude, verzuimfraude, valsheid in geschrifte, verzekeringsfraude en intern onderzoek naar bedrijfsfraude.

GECERTIFICEERD, SNEL EN INTEGER

Wij werken volgens de privacy gedragscodes en beschikken over de benodigde vergunningen en certificeringen. Tevens worden onze onderzoekers geregeld getoetst op hun kennisniveau en integriteit. Onderzoek vindt plaats met inachtneming van de laatste normeringen, waardoor de verkregen informatie als rechtmatig verkregen bewijs kan worden ingezet.

MODERNE APPARATUUR

Iedereen laat digitale sporen achter op diverse soorten digitale gegevensdragers, denk hierbij aan een mobiele telefoon, iPad, laptop, pc en server.

Onze specialisten gebruiken deze sporen voor doelgericht forensisch onderzoek. Hierbij beschikken wij over de modernste apparatuur. Maar ook onze ontwikkelde internet monitoring tools en jarenlange expertise zijn onmisbaar.

INTERNET RECHERCHEURS

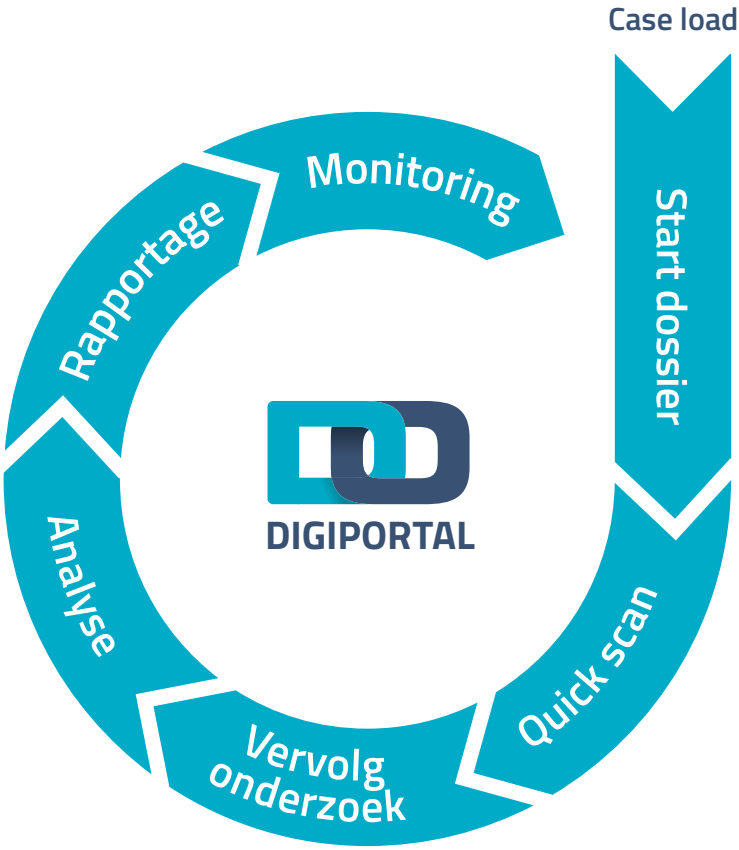
Onze rechercheurs zijn gespecialiseerd in het naar boven halen van waardevolle informatie op het internet. Dit doen we via openbare bronnen zoals zoekmachines en social media, maar ook via het gedeelte van het internet dat ver weggestopt en moeilijk benaderbaar is. De diverse bronnen vragen om verschillende soorten opsporingsmiddelen en werkwijzen.

HET STAPPENPLAN

Wij bieden u de mogelijkheid om digitaal onderzoek volgens een standaard stappenplan uit te voeren. Daarbij maken wij gebruik van een onderzoeksportaal waarin u continu inzicht heeft in de analyses en rapportages. Na iedere fase vindt er een 'go'/'no go'-moment plaats.

VOORDELEN VAN DO DIGIPORTAL

- Betrouwbaar (encrypt) communiceren;
- Alle dossierinformatie wordt centraal beheerd;
- Voortgang van onderzoek eenvoudig te monitoren;
- Veilig down- & uploaden van privacy-gevoelige informatie;
- Methodiek binnen kaders van wetgeving POB 1182.



CYBER SECURITY

GEVAREN VAN HET INTERNET

Het internet biedt veel mogelijkheden, kansen en voordelen. Dit heeft echter ook een keerzijde: we worden kwetsbaar en afhankelijk. Systemen worden gehackt en door datalekken komen belangrijke documenten ongewild op straat te liggen. Er is een trend zichtbaar waarin organisaties steeds vaker het doelwit van cybercriminelen zijn.

BESCHERMING PRIVACY

De bescherming van de privacy is in verschillende wetten en verdragen geregeld. Het gaat hier bijvoorbeeld om het verwerken van persoonsgegevens. Het niet naleven van de regelgeving kan tot hoge boetes van de overheid leiden.

In lijn met de nieuwe Europese dataprotectie wetgeving mogen bedrijven alleen onder strikte voorwaarden persoonlijke informatie verzamelen en bewaren. Deze privacyverordening verplicht organisaties een data protection officer, oftewel een functionaris gegevensbescherming, aan te stellen.

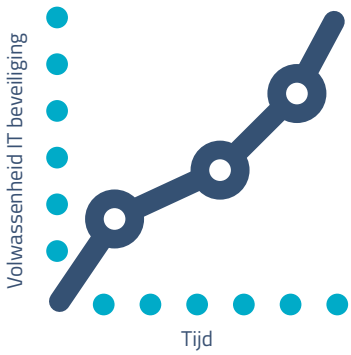
DESKUNDIG, ERVAREN EN INTEGER

Wij zijn gespecialiseerd in internet onderzoek, cyber security en IT auditing. Samen met u zorgen we ervoor dat uw organisatie een sterk verminderde kans heeft op imagoschade, boetes door de overheid of hoge herstelkosten als gevolg van cybercriminaliteit. Wij toetsen en verbeteren uw informatiebeveiliging en besteden aandacht aan bewustwording binnen uw organisatie.

ONZE METHODIEK

De methode waarvan we gebruik maken bij cyber security is een continu repeterend proces. Hierdoor blijft de informatiebeveiliging altijd optimaal en up-to-date en loopt uw organisatie een zo laag mogelijk risico.

De projectmatige aanpak in combinatie met een op uw organisatie toegespitst verbetertraject én onze gespecialiseerde auditors zorgen ervoor dat uw cyber security op een steeds hoger niveau komt te liggen.



HET CYBER SECURITY-CONCEPT

Het Cyber Security-concept start met een (nul)meting. Dit is een analyse van de actuele situatie, waarin het beveiligingsbeleid van uw bedrijf en het bewustzijn van digitale veiligheid van uw medewerkers wordt meegenomen. Op basis hiervan wordt een plan van aanpak voorgesteld met de te treffen maatregelen.

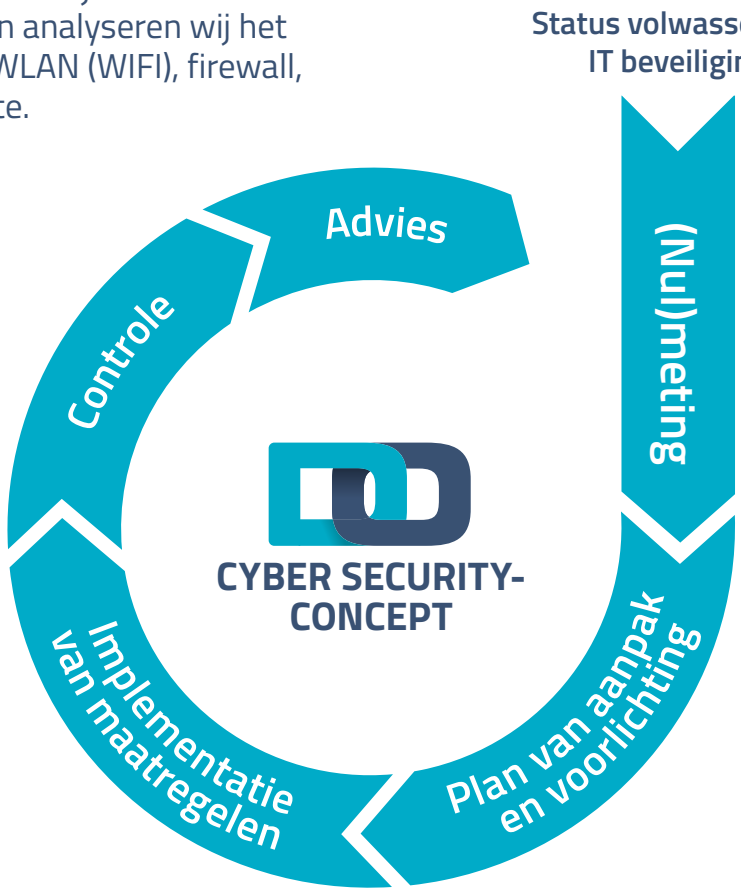
VOORDELEN VAN HET CYBER SECURITY-CONCEPT

- Op basis van de implementatie van een doordacht informatiebeveiligingsbeleid, vermindert de kans dat uw organisatie schade ondervindt van cyber-criminaliteit en/of datalekken aanzienlijk.
- Op basis van jarenlange ervaring hebben wij trainingsmethodieken ontwikkeld die de bewustwording van uw medewerkers betreffende de gevaren van cybercriminaliteit significant verbetert. Hierdoor worden risico's van datalekken sterk gereduceerd.

Daarnaast verrichten wij eventuele 'phishing' audits en analyseren wij het functioneren van WLAN (WIFI), firewall, netwerk en website.

Na de (nul)meting vindt het verbetertraject plaats. Dit traject omvat:

- Invoering van voorgestelde maatregelen;
- Een periodieke check van uw internet-omgeving;
- Handhaving van het cyber security-beleid;
- Bewustwording van uw personeel ten aanzien van digitale veiligheid.



OPLEIDINGEN

WAAROM IS TRAINING BELANGRIJK?

De internettechnologie is continu in ontwikkeling. Om uw kennis op het gebied van digitaal forensisch onderzoek en cyber security actueel te houden, bieden wij een breed scala aan trainingen en opleidingen aan. Hiermee beperkt u de gevaren die het internet met zich meebrengt en weten u en uw medewerkers de kansen die er liggen optimaal te benutten.

DE BESTE OPLEIDERS EN FACILITEITEN

De opleidingen die wij aanbieden worden altijd verzorgd door experts binnen het vakgebied. De experts beschikken over de gewenste didactische vaardigheden en maken gebruik van kwalitatief hoogwaardig lesmateriaal. Daarnaast hebben we een eigen DO Academie, die uitermate geschikt is voor het faciliteren van de verschillende trainingen.

OPEN INSCHRIJVING OF INCOMPANY

Wij bieden de opleidingen zowel als open inschrijving als op incompany basis aan. Bij de open inschrijving staan trainingsinhoud, -data en –tijden vast. Medewerkers van verschillende bedrijven nemen aan deze training deel.

OPLEIDING OP MAAT

Voor de incompany cursussen is maatwerk mogelijk. De geschetste trainingen zijn slechts voorbeelden van de mogelijkheden die wij te bieden hebben. Met onze maatwerktrainingen zijn wij in staat om een training volledig aan te laten sluiten bij uw wensen en behoeften.

Voorbeelden maatwerk trainingen:

Osint, Open-source intelligence training.
Doelgroep fraude onderzoekers, politie, marechausse

Fosint, Financieel rechercheren op het internet.
Doelgroep Accountants.

Internet Screening voor HR Professionals.
Doelgroep HR Managers

Security Analyst & Licensed Penetration Tester.
Doelgroep Security Professionals.

EEN BREED SCALA AAN OPLEIDINGEN

ZOEKEN OP INTERNET – 1 DAG

Wij trainen deelnemers in de basistechnieken van het zoeken naar personen en bedrijven op het internet met behulp van openbare bronnen. In onze training houden we rekening met de veiligheid, juridische kaders en de privacywetgeving. Deelnemers ontwikkelen vaardigheden en doen kennis op die ze kunnen gebruiken in hun dagelijks werk.

INTERNET RECHERCHEREN – 2 DAGEN

In deze training hebben we extra aandacht voor de digitale forensisch component en uitgebreide casuïstiek. In dit kader worden deelnemers getraind in technieken die ze in staat stellen om, met behulp van openbare bronnen, te zoeken naar personen en bedrijven op het internet.

DIGITAL SECURITY AWARENESS TRAINING – 1 DAGDEEL

In deze interactieve workshop trainen we uw medewerkers om de risico's die het internet met zich meebrengt, te beperken. Aan de hand van praktijkvoorbeelden voeren deelnemers handelingen op de computer uit die ze bewust maken van de gevaren van het internet. Daarnaast laten we de mogelijkheden zien die het internet biedt.

INTERNET AWARENESS – E-LEARNING

In deze training, die volledig naar uw wensen wordt samengesteld, maken wij uw personeel cyber-proof. In de vorm van e-learning maken wij uw organisatie bewust van de gevaren die het internet met zich meebrengt. Op deze manier beperkt u een aantal risico's en gevaren. De training kan ook worden gecombineerd met een face-to-face trainingsvariant.

INTERACTIEVE SESSIE CYBERCRIME

In onze 45 minuten durende interactieve sessie cybercrime komen een aantal onderwerpen aan bod die u en uw medewerkers bewust maken van de gevaren en mogelijkheden van het internet.

- Wat is cybercrime?
- De voor- en nadelen van social media;
- Een live-demonstratie van wat er allemaal mogelijk is met een smartphone;
- Methodes om op een eenvoudige manier onderzoek te verrichten naar de betrouwbaarheid van bedrijven en personen.

Digitale Opsporing

Digitale Opsporing is een door het ministerie van Veiligheid en Justitie erkend particulier digitaal forensisch recherchebureau en cyber security specialist.

Digitale Opsporing lost uw vraagstuk snel en integer op door het verzamelen, verwerken en nauwkeurig analyseren van digitale sporen en gegevens. Wij garanderen hierbij discretie en stellen de data binnen uw organisatie veilig.

Naast het onderzoeken, adviseren wij u over het voorkomen en bestrijden van cybercrime en mogelijke datalekken. Wij bieden u meerdere trainingen en opleidingen aan vanuit onze academie.

Digitale Opsporing voorkomt en bestrijdt digitale criminaliteit. Wij geven u de inzichten die u nodig heeft en optimaliseren uw veiligheid!

Contactgegevens:
Digitale Opsporing BV
Nijverheidsstraat 8
5961 PJ Horst
085-489 12 50
www.DigitaleOpsporing.nl