DataExpert Academy

Overzicht **trainingen**

Digital Forensics
Data Analytics
OSINT
Cryptocurrency
Cybercrime
Cyber Security

Betekenis symbolen

- Klassikale training
- Online training
- SPEN geaccrediteerd

- Nederlandse training
- Engelse training

Als expert op het gebied van technologie voor analyse & visualisatie, digital forensics, incident response en cyber security biedt DataExpert ook specialistische, up-to-date trainingen. DataExpert geeft trainingen op productniveau, maar ook op het gebied van cybercrime, cyber security, OSINT en cryptocurrency. Daarnaast zijn trainingen op maat en on the job mogelijk. Verder beschikt DataExpert over een CRKBO accreditatie, zijn enkele trainingen SPEN-geaccrediteerd en hebben onze docenten jarenlange kennis & ervaring uit de praktijk.

Om het beste uit uzelf te halen en uit tools waarmee u dagelijks werkt, is training essentieel. De trainingen van DataExpert zorgen ervoor dat u vertrouwd en zelfverzekerd aan de slag kunt gaan. In ons moderne trainingscentrum in Veenendaal verzorgen we onze trainingen, maar we kunnen ook trainingen inclusief laptops en trainingsmateriaal op locatie of online geven. Daarnaast wordt een groot deel van onze trainingen ondersteunt door het e-learning platform van DataExpert.

Neem voor meer informatie over de trainingsmogelijkheden contact met ons op.

Inhoudsopgave

DataExpert

Analytics

De diversiteit, volume en snelheid waarmee data en criminaliteit zich ontwikkelen verhogen de complexiteit in het bestrijden van criminaliteit aanzienlijk. Zowel het verkennen en interpreteren van data als het vinden van verbanden/connecties tussen entiteiten wordt steeds moeilijker. Het uitvoeren van diepgaande analyses, maar ook het toevoegen van informatie afkomstig uit verschillende offline of online digitale databronnen, zoals Dark/DeepWeb en Social Media, zijn essentiële stappen in het analyseproces.

De Analytics trainingen zorgen voor inzicht en vaardigheden op het gebied van data-analyse, waarbij er gebruik wordt gemaakt van verschillende technologieën. Dit met als doel dat de juiste intelligentie uit data wordt gehaald om een criminaliteitsdossier op te lossen.

Analytics

i2 Analyst's Notebook

Tijdens deze vierdaagse training leert u hoe u i2 Analyst's Notebook als hulpmiddel kunt gebruiken bij het oplossen van grotere vraagstukken zoals 'Zoek uit of er een verband bestaat tussen een reeks inbraken en een reeks telefoongesprekken'. De voorbeelden en vraagstukken komen uit de politiepraktijk (autodiefstal, mensenhandel, drugstransporten, moord en beroving) en uit de financiële sector (financiële fraude, identiteitsfraude, skimming, vervalsing, witwaspraktijken).

Voor wie is deze training bedoeld?

De training is bedoeld voor onderzoekers en analisten die zich bezig (gaan) houden met het visualiseren en (diepgaand) analyseren van onderzoeksgegevens (voor tactische, strategische of operationele analyse).
i2 Analyst's Notebook wordt (meestal in combinatie met i2 iBase User) vooral gebruikt door analisten van de politie, defensie, grote particuliere- of overheidsorganisaties, banken, non-profits en verzekeringsmaatschappijen.
Deze training is ook uitermate geschikt voor (aankomende) studenten van de cursus Analyseren van Informatie (AvI) van de Politieacademie.

Wat leert u tijdens de training?

- Handmatig relatieschema's maken en opmaken
- Handmatig tijdlijnen maken en opmaken, met en zonder gebeurtenisvensters
- Het toevoegen van kaarten en attributen op relatieschema's
- Verschillende lay-out vormen toepassen voor zowel relatieschema's als tijdlijnen
- Importeren van .txt en .xls bestanden naar relatieschema's en tijdlijnen
- Een schema controleren op dubbele records en vervolgens samenvoegen, koppelen of uitsluiten
- Een schema analyseren met behulp van List Items
- Een schema doorzoeken met de functies Search, Find Text en Visual Search
- Een schema doorzoeken, filteren en de gefilterde informatie naar een nieuw schema kopiëren met barcharts, histogrammen en heatmaps
- Een voorwaardelijke opmaak maken van een schema om bepaalde elementen in één oogopslag uit te lichten door te vergroten/andere kleur/etc.
- Een netwerk van personen/telefoons/bankrekeningen/ analyseren met de sociale netwerk analyse tool

Let op: Wij adviseren om deze training voorafgaand aan de iBase User training te volgen.

DataExpert

i2 iBase User

Tijdens deze training leert u relationele databases te gebruiken waarin alle gegevens kunnen worden ingevoerd, zowel handmatig als via een import, die relevant zijn voor uw onderzoek. Tevens leert u ook de data doorzoeken en analyseren middels Browse, Find, Queries, Search 360, Scored Matching, Sets creëren en data (naar Analyst's Notebook) exporteren.

Met het programma i2 iBase User kunt u onderzoeksgegevens uit allerlei verschillende bronnen en met verschillende formats op een relationele wijze opslaan, doorzoeken en visualiseren. In combinatie met i2 Analyst's Notebook is het mogelijk om deze data verder te analyseren. In deze vierdaagse training leert u hoe i2 iBase User als hulpmiddel kan worden gebruikt bij het oplossen van vraagstukken zoals 'Zoek uit of de personen die aan het persoonsprofiel voldoen elkaar mogelijk kennen'. De voorbeelden en vraagstukken komen uit de politiepraktijk (autodiefstal, mensenhandel, drugtransporten, moord en beroving) en uit de financiële sector (financiële fraude, identiteitsfraude, skimming, vervalsing, witwaspraktijken).

De training bestaat uit een training van drie dagen en een refresherdag een aantal weken later. Op deze manier kunt u een praktijkvraagstuk inbrengen en meer tips en tricks aanleren die aansluiten bij uw dagelijkse werkzaamheden.

Voor wie is deze training bedoeld?

De training is bedoeld voor onderzoekers en analisten die zich bezig (gaan) houden met het invoeren, analyseren en visualiseren van onderzoeksgegevens op een relationele manier (voor tactische, strategische of operationele analyse). i2 iBase User wordt (meestal in combinatie met i2 Analyst's Notebook) vooral gebruikt door analisten van de politie, defensie, grote particuliere- of overheidsorganisaties, banken, non-profits en verzekeringsmaatschappijen.

Wat leert u tijdens de training?

- Nieuwe records aanmaken door gegevens handmatig in te voeren in de velden van entiteiten en koppelingen.
- Weergeven van de records, vergelijken, sorteren en zoeken naar dubbele gegevens.
- Uitgebreid zoeken in de gegevens, met o.a. Browse, Queries, Search 360 en Scored Matching.
- Gegevens invoeren met datasheets, waardoor de invoer van gegevens efficiënter en minder foutgevoelig wordt.
- Records importeren uit een tekstbestand of uit een andere toepassing zoals MS Excel of MS Access.
- Grote aantallen records bewerken of wissen.
- Sets maken en analyseren.
- Records exporteren.
- Gegevens weergeven en koppelingen onderzoeken in een i2 iBase Link Chart en in i2 Analyst's Notebook.
- Werken met relevante i2 Analyst's Notebook tools en opties met betrekking tot de koppeling met i2 iBase, bijvoorbeeld tijdlijnen genereren in i2 Analyst's Notebook en expanderen.

Let op: Wij adviseren om deze training na de i2 Analyst's Notebook training te volgen

i2 iBase Designer

Met i2 iBase Designer ontwerpt u relationele databases waarin alle gegevens kunnen worden ingevoerd die relevant zijn voor uw onderzoek. In de zomer van 2023 zijn we gestart met een andere vormgeving van de iBase Designer training. De training is specifiek gericht op alles wat komt kijken bij het maken van een database. Van het ontwerpen tot het onderhouden van een database.

Tijdens deze training leert u hoe u in i2 iBase databases kunt ontwerpen die aansluiten bij de behoeften van analisten. Hiermee beantwoordt u vragen als 'welke entiteiten en koppelingen moeten er in de database komen', 'van welk type moeten de velden zijn', 'hoe activeer ik verschillende zoekfuncties' en 'hoe ken ik gebruikersrechten toe'. De voorbeelden en vraagstukken komen uit uiteenlopende werkvelden met diverse soorten en vormen van data, waaronder financiële gegevens, telecomgegevens, ICT-gegevens, forensische gegevens en persoonsgegevens.

De training bestaat uit een training van drie dagen en een refresherdag een aantal weken later. Op deze manier kunt u een praktijkvraagstuk inbrengen en meer tips en tricks aanleren die aansluiten bij uw dagelijkse werkzaamheden.

Voor wie is deze training bedoeld?

De training is bedoeld voor database ontwerpers en analisten die zich bezig (gaan) houden met het ontwerpen, maken (en beheren) van een relationele database. In de praktijk wordt i2 iBase Designer (meestal in combinatie met i2 Analyst's Notebook) vooral gebruikt door analisten van de politie, defensie, grote particuliere- of overheidsorganisaties, banken, non-profits en verzekeringsmaatschappijen.

Bij aanvang van deze training wordt verwacht dat u de nodige kennis heeft van iBase User. Om een goede database te kunnen maken is het van belang om te weten wat de gebruiker nodig heeft. Om de ontworpen database te kunnen testen is het nodig om te weten hoe u records kan invoeren, documenten kan importeren en weet hoe u de database kan raadplegen.

Wat leert u tijdens de training?

- Uitdenken van een relationeel datamodel
- Ontwerpen van een i2 iBase database, met daarbij meerdere mogelijkheden voor Security en Audit Levels
- Creëren van de i2 iBase database op basis van dit ontwerp
- Entiteiten en koppelingen aanmaken met bijbehorende semantische betekenissen
- Verschillende typen velden aanmaken, waaronder rekenvelden, discriminator velden, index velden en standaardvelden
- Bijlagen, gradaties van zekerheid aan velden toevoegen
- Word search en search 360 indexeren
- Labeling schema's en Schema-attributen aanmaken
- Datasheets ontwerpen waardoor de invoer efficiënter en minder foutgevoelig wordt

- Records importeren uit gestructureerde data formats.
- Bouwen, schedulen en opslaan voor hergebruik van deze importspecificaties
- Een template maken van een database en een database maken aan de hand van een template
- Een database repareren, comprimeren, beheren en controleren
- Een database beheren en beveiligen

Let op: Deze training gaat alleen in op het ontwerpen van databases en niet op het gebruik. i2 iBase User kennis wordt als voorkennis verwacht voor deelname aan deze training.

Applicatie Management voor i2 iBase en i2 Analyst's Notebook

De vragen waar functioneel beheerders tegenaan lopen bij het inrichten en beheren van de i2 iBase en i2 Analyst's Notebook producten heeft DataExpert verwerkt tot een eendaagse training waarin veelgestelde vragen worden beantwoord en de technische aspecten van i2 iBase en i2 Analyst's Notebook worden belicht.

Voor wie is deze training bedoeld?

Functioneel beheerders die inzicht willen krijgen in:

- Hoe richt ik i2 iBase & i2 Analyst's Notebook in op het netwerk?
- Welke functies zijn beschikbaar?
- Hoe ga ik om met back-ups?

Wat leert u tijdens de training?

i2 iBase:

- Security files en databases, Access en SQL server databases, file extensies, SQL server clients servers en netwerk, user profile informatie, optionele paden voor gebruikers.
- Autorisatiebeheer: rechten op de database, security files, gebruikers en groepen, het gebruik van SCC codes.
- Databases: creëren van databases via templates, creëren van een case-controlled database, gebruik van subsets. Soft delete, batch delete, SQL server connectie settings, verplaatsen SQL server databases. Welke bestanden vereisen een back-up, update database schema, schema en link integrity check en plug-ins.
- Setup en gebruik van de extra functies: alerting, search 360, installatie op SQL Server en Client, SQL Server Agent, auditing, iBase Scheduler voor batch imports en exports, bulk import.

i2 Analyst's Notebook:

- Optionele paden voor gebruikers.
- Plug-ins.
- Eigen icoontjes en templates.
- Importspecificaties en batch imports.
- Spellingchecker en tijdlijn in Nederlands datumformaat.

Extra informatie

Deze training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

Mercure

Mercure is een unieke software oplossing en de facto standaard in meerdere landen op het gebied van complexe telecom analyse. Het biedt u de mogelijkheid om CDR's, zendmastgegevens, forensische mobiele extracties van diverse formaten en iOS-versies moeiteloos samen te voegen met tap- en peilbakengegevens waarbij de data wordt ontdubbeld. Binnen seconden kunt u tevens online communicatie data zoals WhatsApp en Snapchat snel doorzoeken, waarbij alles automatisch geografisch en/of in een tijdlijn omgezet kan worden. Volg deze tweedaagse training en leer alle ins en outs van Mercure.

Voor wie is deze training bedoeld?

De Mercure training is bedoeld voor onderzoekers, telecom rechercheurs en operationele analisten.

Wat leert u tijdens de training?

DataExpert biedt deze producttraining aan om gebruikers alle onderdelen van Mercure eigen te laten maken. Er zal worden ingegaan op het inlezen van gegevens maar ook op de grote hoeveelheid ingebouwde zoekopdrachten, tijdlijnen, gespecialiseerde queries en grafische weergaven. Door middel van praktijkgerichte casussen wordt de gebruiker meegenomen in alle mogelijkheden die Mercure te bieden heeft.

Extra informatie

Deze training kan in het Nederlands of Engels worden verzorgd.

DataExpert

SINTELIX User Training for i2 Analyst's Notebook

Tijdens deze training leren cursisten uitgebreide analyse en visualisatie technieken voor grote volumes ongestructureerde data met behulp van SINTELIX. SINTELIX extraheert, analyseert en visualiseert entiteiten, relaties en andere belangrijke informatie uit grote hoeveelheden tekstdata. Accuratesse en hoge performance zijn twee redenen waarom opsporingsdiensten wereldwijd voor SINTELIX hebben gekozen.

Voor wie is deze training bedoeld?

Deze vijfdaagse training is geschikt voor operationele/zaaksanalisten, digital rechercheurs en strategische/tactische analisten die tijdens hun onderzoeken gebruikmaken van i2 software.

Wat leert u tijdens de training?

- Link, entiteit en metadata extractie met SINTELIX.
- Netwerk semantische -, geografische - en tijdsanalyse met behulp van SINTELIX.
- Uitgebreide search/zoekfilters te gebruiken, inclusief het clusteren van zoekresultaten volgens verschillende criteria.
- De geëxtraheerde gegevens interactief te benaderen en aan elkaar te koppelen.
- Onderzoeksdata en analyse in i2 Analyst's Notebook te verreiken met nieuwe inzichten uit ongestructureerde data.
- Alle geëxtraheerde gegevens interactief te benaderen en aan elkaar te koppelen.

Extra informatie

Deze training is in het Engels en kan zowel klassikaal als online worden verzorgd.

Social Network Harvester

Tijdens deze tweedaagse training leert u hoe u Social Network Harvester (SNH) als hulpmiddel kunt gebruiken bij het verzamelen en analyseren van sociale netwerkgegevens tijdens uw onderzoek. Binnen de gebruiksvriendelijke interface van SNH kunt u gebruikmaken van uitgebreide analyse en visualisatie functionaliteiten op het gebied van connecties, berichten, afbeeldingen, video's, opmerkingen en 'likes'. Zo identificeert u op snelle en efficiënte wijze belangrijke netwerkelementen en voorheen onbekende groepen en connecties. Aanvullend leert u tijdens de training het netwerk of delen daarvan te exporteren en veilig te stellen voor verdere verwerking.

De training wordt gegeven op interactieve wijze, waarbij theorie en praktijk met elkaar worden afgewisseld. Onderwerpen worden toegelicht, waarna de deelnemers dit zelfstandig of in duo's oefenen door middel van opdrachten of cases.

Voor wie is deze training bedoeld?

Voor officiële opsporingsinstanties, zakelijke adviesbureaus, advocatenkantoren of recherchebureaus die vanuit een formeel onderzoek meer inzicht willen krijgen in sociale netwerken en onderlinge connecties willen

visualiseren en analyseren. Hierbij bestaat de behoefte om gegevens te verzamelen voor verdere analysedoeleinden.

Wat leert u tijdens de training?

- Het efficiënt onderzoeken van Sociale Netwerken als Facebook, Twitter, Instagram, VKontakte, Odnoklassniki, YouTube, Telegram, TikTok en GETTR.
- Het werken met de Profile Manager i.c.m. de onderzoek accounts.
- Verzamelen/scrapen van gegevens en veiligstellen van vriendenlijsten, groepsleden, fotoalbums en berichten op een tijdslijn inclusief reacties en likes.
- Optimaal gebruikmaken van alle dashboardfunctionaliteiten.
- Analyseren van de verzamelde data, door het vaststellen van een user ID, het identificeren van relevante profielen, het inzichtelijk maken van gedeelde contacten, groepen en activiteiten, en het gereedmaken van de data voor export en verdere analyse.
- Het visualiseren van netwerkdelen en het veiligstellen van relevante netwerkdata.
- Het werken met de rapportagetool.

Extra informatie

Deze training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

Refresher Training

De tijdens een cursus opgedane kennis en vaardigheden zakken weg wanneer de cursist niet direct na de training in de gelegenheid is om aan de slag te gaan met het programma. Een Refresher training is een uitstekende mogelijkheid om kennis en vaardigheden in korte tijd weer op te halen en eventueel kennis te maken met nieuwe versies van dezelfde oplossingen.

Refresher Training i2 Analyst's Notebook of i2 iBase

Fris de belangrijke punten uit de training(en) i2 Analyst's Notebook en i2 iBase op en zet deze kennis en software in voor het oplossen van opsporings- en operationele analyse vraagstukken.

DataExpert

Notities

Notities

Cryptocurrency

Blockchain en cryptocurrencies krijgen een steeds prominentere rol in de samenleving. De verschillende soorten blockchaintechnologieën bieden de mogelijkheid tot ongekende ontwikkelingen; snelle cross-border transacties, verkoop van digitale kunst, decentralized supercomputers en meer. Met de juiste analysemethodes kan inzicht verkregen worden in de wereld van blockchains en kunnen cryptocurrency transacties worden getraceerd en gevisualiseerd.

Tijdens de Cryptocurrency trainingen van DataExpert worden onderzoekers en rechercheurs opgeleid tot cryptocurrency onderzoekers. Verder biedt DataExpert als Gold Partner van Chainalysis naast haar eigen trainingen ook Chainalysis trainingen aan.

Cryptocurrency

Cryptocurrency Investigations

Cryptocurrency en de blockchain ontwikkelen zich razendsnel. Een onderzoek hiernaar uitvoeren brengt daarom vele kansen en uitdagingen met zich mee. Maar hoe werkt dit proces? Tijdens de training “Cryptocurrency Investigations” leren de deelnemers alle ins & outs omtrent cryptovaluta en de blockchain. De cursisten leren onderzoek uit te voeren vanuit meerdere invalshoeken en met verschillende open source en betaalde tools. Zo kunnen ze na afloop van de training onder meer een Bitcoin transactie volgen en gebruikers de-anonimiseren. Daarnaast zijn ze in staat hun bevindingen te rapporteren.

Voor wie is deze training bedoeld?

Deze vierdaagse training is voor eenieder die (opsporings)onderzoek doet in de blockchain en cryptocurrency. De training is geschikt voor o.a. rechercheurs bij de politie en overige opsporings- en veiligheidsdiensten, thema-onderzoekers, financiële instellingen (CDD, KYC, AML), particulier onderzoekers etc.

Wat leert u tijdens de training?

Aan het einde van deze training hebben de deelnemers inzicht in de mogelijkheden en uitdagingen van cryptovaluta en de blockchain. De deelnemers hebben kennis opgebouwd over alle aspecten (zowel technische als de sociale aspecten) van cryptocurrency en de blockchain. Ook kunnen ze na afronding van de training dit onderzoeken en analyseren met behulp van open source tools.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online. Verder is de training modulair opgebouwd waardoor het ook mogelijk is om een maatwerk training samen te stellen met bijpassende casuïstiek.

Cryptocurrency Investigations - Expert (maatwerk)

Tijdens het uitvoeren van een onderzoek naar blockchains en cryptocurrencies zijn er buiten de conventionele onderzoeksmethodes ook geavanceerde methodes toe te passen met of zonder analyse tooling.Naast onze standaard trainingen biedt DataExpert tevens Cryptocurrency Investigations Expert trainingen op maat aan. Hierbij wordt samen met onderzoeksteams gekeken naar de wensen en behoeften en wordt de training afgestemd op het vakgebied van de deelnemers.
Aangezien het niveau van deze training expert is, dienen deelnemers kennis te dragen omtrent de basisonderzoeksmethodes van blockchaintechnologie en cryptocurrencies. Daarnaast is het vereist dat de deelnemers minimaal drie maanden onderzoekservaring hebben op het gebied van blockchains en cryptocurrencies.

De duur van de training is afhankelijk van de vooraf besproken behoeften van de deelnemers en het aantal cursisten. Verder kan de training in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

DataExpert

Ethereum Basics

De ontwikkelingen van cryptocurrencies en blockchain gaan razendsnel. De Ethereum blockchain is daarbij onmiskenbaar naast Bitcoin uitgegroeid tot een van de meest gebruikte. Een onderzoek op de Ethereum blockchain biedt hierom veel kansen voor onderzoekers, maar ook nieuwe uitdagingen. Hoe kan de onderzoeker hier mee om gaan?

Tijdens de training “Ethereum Basics” leren de deelnemers alle ins & outs omtrent de Ethereum Blockchain. De cursisten leren onderzoek uit te voeren vanuit meerdere invalshoeken en met verschillende open source tooling. Zo kunnen ze na afloop van de training onder meer Ethereum transacties, swaps en staking en lending volgen en gebruikers de-anonimiseren. Daarnaast zijn ze in staat hun bevindingen te rapporteren.

Voor wie is deze training bedoeld?

Deze tweedaagse training is voor eenieder die (opsporings)onderzoek doet in de blockchain en cryptocurrency. De training is geschikt voor o.a. rechercheurs bij de politie en overige opsporings- en veiligheidsdiensten, thema-onderzoekers, financiële instellingen (CDD, KYC, AML), particulier onderzoekers etc.

Wat leert u tijdens de training?

Aan het einde van deze training hebben de deelnemers inzicht in de mogelijkheden en uitdagingen van de Ethereum blockchain. De deelnemers hebben kennis opgebouwd over de meest belangrijke basisaspecten (zowel technische als de sociale aspecten) van deze blockchain alsmede de werking en uitvoering van smart contracts. Ook kunnen ze na afronding van de training dit onderzoeken en analyseren met behulp van open source tools.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online. Verder is de training modulair opgebouwd, waardoor het ook mogelijk is om een maatwerk training samen te stellen met bijpassende casuïstiek.

Ethereum Advanced

De Ethereum blockchain heeft een boost gegeven aan adoptie waaruit meerdere protocollen en EVM-compatible chains zijn ontstaan. Hoe kan de onderzoeker met de vele kansen en uitdagingen om gaan?

Tijdens de training “Ethereum Advanced” leren de deelnemers alle ins & outs omtrent Ethereum protocollen en EVM-compatible blockchains zoals chainhopping, privacy protocollen en meer. De cursisten leren onderzoek uit te voeren vanuit meerdere invalshoeken en met verschillende open source tooling. Zo kunnen ze na afloop van de training onder meer cross-chain transacties volgen, de mogelijkheden herkennen in het traceren van privacy transacties en NFT transacties onderzoeken. Daarnaast zijn ze in staat hun bevindingen te rapporteren.

Voor wie is deze training bedoeld?

Deze tweedaagse training is voor eenieder die (opsporings)onderzoek doet in de blockchain en cryptocurrency. De training is geschikt voor o.a. rechercheurs bij de politie en overige opsporings- en veiligheidsdiensten, themaonderzoekers, financiële instellingen (CDD, KYC, AML), particulier onderzoekers etc.

Wat leert u tijdens de training?

Aan het einde van deze training hebben de deelnemers inzicht in de mogelijkheden en uitdagingen van de verschillende geavanceerde aspecten van de Ethereum en andere EVM-compatible blockchains. De deelnemers hebben kennis opgebouwd over alle aspecten (zowel technische als de sociale aspecten) van deze blockchains en de cryptocurrencies hierop ontwikkeld. Ook kunnen ze na afronding van de training dit onderzoeken en analyseren met behulp van open source tools.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online. Verder is de training modulair opgebouwd, waardoor het ook mogelijk is om een maatwerk training samen te stellen met bijpassende casuïstiek

Chainalysis Cryptocurrency Fundamentals (CCFC)

Tijdens de training “Chainalysis Cryptocurrency Fundamentals (CCFC)” leren de deelnemers de fundamentele kennis omtrent blockchaintechnologie en cryptocurrency. Vervolgens leren de deelnemers aan de hand van deze kennis de blockchain explorers te benutten tijdens het onderzoeken van Bitcoin transacties.

Voor wie is deze training bedoeld?

De Chainalysis Cryptocurrency Fundamentals Certification (CCFC) training is geschikt voor eenieder zonder basiskennis van cryptocurrency en blockchain technologie. Deelnemers kunnen afkomstig zijn van onder meer de Nationale Politie en overige opsporings- en veiligheidsdiensten, financiële instellingen (CDD, KYC, AML), particulier onderzoekers en meer.

Wat leert u tijdens de training?

Aan het einde van deze vierdaagse training (vier dagdelen) kan de deelnemer de waarde en context van cryptocurrency herkennen in relatie tot het traditionele financiële systeem. De deelnemer heeft de onderliggende techniek van blockchaintechnologie geleerd waarop cryptocurrencies werkzaam zijn. Hij/zij weet na afloop hoe Bitcoin werkt en heeft kennis opgebouwd over de meest gebruikte Altcoins. Daarnaast kan hij/zij het ecosysteem evalueren, key actors identificeren en is hij/zij op de hoogte van de regulering en privacy ontwikkelingen. Met de vergaarde kennis is de deelnemer in staat om basis blockchainanalyses te uitvoeren.

Examen

De deelnemer dient een examen af te leggen en een score van minimaal 75% te behalen. Het examen wordt afgenomen aan het einde van dag vier. Deze training biedt alle kennis om het examen met succes af te ronden.

DataExpert

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

Cryptocurrency Investigations Basics & Chainalysis Reactor Certification

Om onderzoek uit te kunnen voeren naar transacties waarbij er gebruik wordt gemaakt van cryptovaluta, is er een solide basiskennis vereist van de werking hiervan. Daarnaast is het kunnen inzetten van een tool die deze transacties kan monitoren en analyseren van belang. Tijdens de training “Cryptocurrency Investigations Basics & Chainalysis Reactor Certification” bouwen de deelnemers basiskennis op omtrent cryptocurrency en de blockchain. Daarnaast leren de cursisten om onderzoek uit te voeren met Chainalysis Reactor, wereldwijd dé tool voor blockchain onderzoeken.

Voor wie is deze training bedoeld?

Deze vierdaagse training is geschikt voor eenieder die (opsporings)onderzoek doet naar de blockchain en cryptocurrency en gebruiker is van Chainalysis Reactor. Denk hierbij aan de politie en overige opsporings- en veiligheidsdiensten, themaonderzoekers, financiële instellingen (CDD, KYC, AML), particulier onderzoekers etc.

Wat leert u tijdens de training?

Aan het einde van deze training hebben de deelnemers inzicht gekregen in de mogelijkheden en uitdagingen van cryptovaluta en de blockchain. De cursisten hebben kennis opgebouwd over de “core-concepts”, minen, wallets, ledger etc. Ook kunnen de deelnemers na afloop van de training de analysetool Chainalysis Reactor gebruiken voor hun onderzoeken en analyses.

Examen

Voor Chainalysis Reactor Certification (CRC) dient de deelnemer een examen af te leggen en een score van minimaal 75% te behalen. Het examen wordt afgenomen aan het einde van dag vier. Deze training biedt alle kennis om het examen met succes af te ronden. Indien nodig is er één herkansing inbegrepen bij de opleiding.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online. Verder is de training modulair opgebouwd, waardoor het ook mogelijk is om een maatwerk training samen te stellen met bijpassende casuïstiek.

Chainalysis Reactor Certification (CRC)

Cryptocurrency en de blockchain ontwikkelen zich razendsnel. De analysetool Chainalysis Reactor biedt de mogelijkheid om de blockchain en cryptovaluta te analyseren en te onderzoeken.

Voor wie is deze training bedoeld?

Deze tweedaagse training is geschikt voor gebruikers van Chainalysis Reactor. Fundamentele kennis van cryptovaluta en transacties in de blockchain is vereist.

Wat leert u tijdens de training?

De deelnemers kunnen aan het einde van deze training de Chainalysis Reactor tool inzetten voor het onderzoeken en analyseren van de blockchain en Bitcoin transacties. Ze hebben een zodanige ervaring opgebouwd dat ze het examen Chainalysis Reactor Certification (CRC) met succes te kunnen voltooien.

Examen

Voor Chainalysis Reactor Certification dienen de deelnemers een examen af te leggen en een score van minimaal 75% te behalen. Het examen wordt afgenomen aan het einde van dag twee. Deze training biedt alle kennis om het examen met succes af te ronden. Indien nodig is er één herkansing inbegrepen bij de opleiding.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

Chainalysis Reactor Certification: Recertify

Na het behalen van Chainalysis Reactor Certification kunt u de juiste werkwijzen en analysemethodes toepassen in onderzoeken naar cryptocurrencies en blockchains. Het werkveld is dynamisch en daarom veranderen de onderzoeksmethodes regelmatig. Door productupdates past Chainalysis Reactor zich hierop aan.
De jaarlijkse Chainalysis Reactor Certification: Recertify training zorgt ervoor dat u op de hoogte blijft van de nieuwste ontwikkelingen en trends. Hierdoor kunt u optimaal gebruik blijven maken van Chainalysis Reactor.

Voor wie is deze training bedoeld?

De Chainalysis Reactor Certification: Recertify training is bedoeld voor gebruikers van Chainalysis Reactor die de Chainalysis Reactor Certification al hebben gevolgd en het examen hebben gehaald.

Wat leert u tijdens de training?

Na afloop van deze eendaagse training heeft de deelnemer zijn/haar kennis opgehaald over de basisfunctionaliteiten van Chainalysis Reactor, zodat hij/zij deze zo optimaal mogelijk kan benutten. Ook heeft de deelnemer geleerd te werken met de nieuwste functionaliteiten van Chainalysis Reactor.

Examen

De deelnemer dient een examen af te leggen en een score van minimaal 75% te behalen. Het examen wordt afgenomen aan het einde van de dag. Bij de training is één herkansing inbegrepen.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

DataExpert

Chainalysis Investigation Specialist Certification (CISC)

Door de groeiende populariteit van cryptocurrency en het toenemende gebruik van privacy technieken zoals Coinjoin mixing zijn geavanceerde onderzoekstechnieken nodig. Tijdens de tweedaagse Chainalysis Investigation Specialist Certification training leren de deelnemers deze geavanceerde onderzoeksmethodieken en workflows. Hierbij maken ze gebruik van de software Chainalysis Reactor. De training bouwt voort op de geleerde methodieken uit de CRC-training. De CISC-training is een praktijkgerichte training waarin de deelnemers de technieken leren toepassen aan de hand van case studies.

Voor wie is deze training bedoeld?

De Chainalysis Investigation Specialist Certification training is geschikt voor “power users” die minstens drie maanden ervaring hebben in Chainalysis Reactor en het CRC-certificaat hebben behaald.

Wat leert u tijdens de training?

- Gebruik te maken van de geavanceerde mogelijkheden in Chainalysis Reactor.
- Uitgebreide transactie analyses toe te passen door gebruik te maken van “all-source” informatie.
- Welke specifieke wallets zijn gebruikt te identificeren.
- Geavanceerde workflows toe te passen om diepgaander te kunnen analyseren dan de traditionele blockchain analyse.
- Transacties te onderzoeken waar gebruik wordt gemaakt van privacy technieken zoals CoinJoin mixing en chain hopping.

Examen

Voor de Chainalysis Investigation Specialist Certification dienen de deelnemers een examen af te leggen en een score van minimaal 75% te behalen. Het examen vindt plaats binnen twee weken na de training. Deze training biedt alle kennis om het examen met succes af te ronden. Indien nodig, is er één herkansing inbegrepen in de opleiding.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

Chainalysis Risk and Regulation Training (CRRT)

Met de komst van cryptocurrency dienen traditionele Anti-Money Laundering (AML) assessment frameworks te worden uitgebreid. Door een risk based approach (RBA) op cryptocurrencies toe te passen kan er een effectief AML/compliance beleid worden uitgevoerd dat voldoet aan de geldende wet- en regelgeving. Tijdens de Chainalysis Risk en Regulation training leren de deelnemers een risk based approach toe te passen en off-chain en on-chain data te analyseren.

Voor wie is deze training bedoeld?

De training is geschikt voor analisten, onderzoekers en zij die toezicht houden op cryptocurrencies dan wel cryptocurrency activiteiten/bedrijven monitoren en/of rapporteren.

Wat leert u tijdens de training?

- Cryptocurrencies van elkaar te onderscheiden (privacy coins, stable coins etc.), risico's te herkennen en te mitigeren.
- De werking van DeFi (Decentralised Finance) en het effectief toepassen van transactiemonitoring.
- Welke geografische overwegingen er gemaakt moeten worden bij transactiemonitoring.
- Blockchain analytics.
- Risico's van VASP's (Virtual Asset Service Providers) te herkennen en te mitigeren. Zowel in de vorm van on-chain als off-chain data.
- Red flags te detecteren van cryptocurrency exchanges door middel van een veilige, door Chainalysis gebouwde, mock cryptocurrency exchange.
- Requirements in het rapporteren in relatie tot ongebruikelijke activiteiten.
- Belangrijke ontwikkelingen in internationale en regionale regelgeving te identificeren en te plaatsen. Compliance beslissingen te evalueren en door middel van een risk based approach conclusies te trekken.

Knowledge Check

Voor het behalen van de Chainalysis Risk and Regulation Certification dienen de deelnemers binnen twee weken na aanvang van de training een knowledge check af te ronden.

Chainalysis Ethereum Investigations Certification (CEIC)

Van alle blockchains die zijn ontwikkeld, is Ethereum nog steeds een van de meest gebruikte blockchains. De analyse tool Chainalysis Reactor biedt de mogelijkheid om deze blockchain en smart contracts die zich hierop hebben gevestigd te onderzoeken. Tijdens de tweedaagseEthereum Investigations Certification training leren de deelnemers de benodigde kennis en werkwijzen om transacties te traceren op de Ethereum blockchain met behulp van Chainalysis Reactor.

Voor wie is deze training bedoeld?

De Chainalysis Ethereum Investigations Certification training is geschikt voor Chainalysis Reactor gebruikers die het CRC-certificaat hebben behaald.

Wat leert u tijdens de training?

- Onderscheid te maken tussen ether transacties en smart contract transacties in Chainalysis Reactor.
- Gecentraliseerde services en smart contracts op Ethereum te identificeren.
- Smart contracts te analyseren door middel van OSINT (Open Source Intelligence).
- De belangrijkste principes op het gebied van Decentralized Finance (DeFi).
- Transactiesporen te volgen door veelgebruikte DeFi protocollen.

Examen

Voor de Chainalysis Ethereum Investigations Certification dienen de deelnemers een examen af te leggen en een score van minimaal 75% te behalen. Het examen vindt plaats binnen twee weken na de training. Deze training biedt alle kennis om het examen met succes af te ronden. Indien nodig, zit er één herkansing inbegrepen in de opleiding.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

TRM Crypto Fundamentals

Deze training geeft inzicht en praktische methoden die nodig zijn om vertrouwd te raken met blockchain-gerelateerde concepten en cryptocurrency. Het is een alomvattende oriëntatie op het crypto-ecosysteem en gerelateerde sleutelconcepten die nodig zijn om cryptocurrency te begrijpen, analyseren en ermee om te gaan, én entiteiten en transacties via blockchains te volgen.

Voor wie is deze opleiding bedoeld?

Deze training is bedoeld voor mensen die niet bekend zijn met cryptocurrency en de blockchain.

Wat leert u tijdens deze opleiding?

- Hoe blockchains en cryptocurrencies werken
- Hoe gegevens gerelateerd aan op blockchain gebaseerde entiteits- of transactieadressen te vinden
- Een transactie volgen via blockchains
- De attributie met betrekking tot dienstverleners, actoren en entiteiten volgen
- Identificeren en gebruiken van open source-attributiemethoden
- Begrijpen van slimme contracten en tokens
- Non-Fungible Tokens (NFT's) uitleggen en hoe deze zich verhouden tot blockchain

TRM Certified Investigator

Naast de grondbeginselen van blockchain-technologie, cryptocurrencies en opkomende gebruiksscenario's, leren studenten on-chain onderzoekstechnieken met behulp van de toonaangevende forensische tools van TRM Lab om de geldstroom te traceren en verdachte activiteiten te koppelen aan entiteiten uit de echte wereld.

Voor wie is deze opleiding bedoeld?

De training is voor iedereen met enige blockchain-onderzoekservaring die crypto-transacties over meerdere blockchains moet traceren.

Wat leert u tijdens deze opleiding?

- Identificeren en verklaren van crypto-misdaadtypologieën
- Gebruik maken van off-chain open source intelligence-bronnen (OSINT).
- Identificeren transactiegegevenstypen
- Begrijpen van blockchain-intelligentiebronnen
- Identificeren van attributie op UTXO en accountgebaseerde blockchains
- Begrijpen van gedragspatronen van blockchain-activiteit door een entiteit
- Traceren van transacties op zowel adresniveau als entiteitsniveau over meerdere blockchains
- Documenteren van transactionele activiteiten in de keten
- Begrijpen van de algemene componenten van crypto-compliance

TRM Advanced Crypto Investigator

TRM-ACI is ideaal voor ervaren gebruikers die blockchain-intelligentie ten volle willen benutten tijdens onderzoeken en biedt mensen uit de praktijk geavanceerde kennis en vaardigheden voor een verscheidenheid aan blockchain-onderzoeksactiviteiten.

Voor wie is deze opleiding bedoeld?

De TRM Advanced Crypto Investigator is een geavanceerde certificeringscursus ontworpen voor mensen met crypto-forensische ervaring.

Wat leert u tijdens deze opleiding?

- Begrijpen van het dreigingslandschap en de vectoren die tot crypto-criminaliteit leiden
- Uitleggen van handmatig demixing via diensten als Wasabi en Tornado Cash
- Begrijpen van afleidingspaden (derivation paths)
- Lezen van contracten en identificeren van contract spoofing
- Toepassen van handtekeningen, zowel handmatig als die beschikbaar zijn in TRM Labs
- Toepassen van geavanceerde forensische methoden, zoals bevestiging van meerdere handtekeningen in hex.

TRM Crypto Compliance Specialist

TRM-CCS biedt de kennis die nodig is om compliance-workflows in de keten te implementeren, de risico's van derden met betrekking tot cryptotransacties te begrijpen en inzicht te krijgen in de huidige trends, typologieën en tooling.

Voor wie is deze opleiding bedoeld?

Compliance- en due diligence-professionals die de vaardigheden nodig hebben om te beschermen tegen misbruik, het witwassen van geld en financiële criminaliteit.

DataExpert

Wat leert u tijdens deze opleiding?

- Begrijpen van het wereldwijde regelgevings- en compliance landschap rond cryptocurrencies
- Identificeren van risicovolle activiteiten op de blockchain en begrijpen hoe deze de risicobereidheid van de organisatie beïnvloeden
- Analyseren van adressen via transactiemonitoring en portemonnee-screening
- Identificeren van externe bewaarders (3PC) en crypto-on- en off-ramps en bepalen hoe ze werken
- Schrijven van effectieve Verdachte Activiteitenrapporten (SAR)

TRM Digital Forensics & Cryptocurrencies

In deze training leert u de fijne kneepjes van blockchain-technologie en het herkennen van cryptocurrency-artefacten die zijn achtergelaten in digitaal bewijsmateriaal, waardoor u de toenemende hoeveelheid onderzoeken met een cryptocurrency-nexus kunt aanpakken.

Voor wie is deze opleiding bedoeld?

Digitale forensische onderzoekers en hun teams die de kloof moeten dichten tussen traditionele digitale forensische onderzoeken en onderzoeken naar cryptocurrency.

Wat leert u tijdens deze opleiding?

- U krijgt inzicht in de fijne kneepjes van blockchain-technologie
- Identificeren van het cryptocurrency-gebruik van individuen en entiteiten
- Herkennen en bewaren van cryptocurrency-artefacten in digitaal bewijsmateriaal
- Begrijpen van de verschillen in populaire soorten cryptocurrency-portefeuilles
- Gebruiken van open-sourcetools voor het analyseren van memory images
- Deconstrueer blockchain-data, waaronder blok- en transactiestructuren

Notities

Cybercrime

Digitalisering is niet meer weg te denken uit onze maatschappij. Zowel privé als zakelijk zijn we meer en meer “connected” en wordt er steeds meer data online opgeslagen en gedeeld. Een goudmijn voor de cybercrimineel die zelf ook steeds eenvoudiger zijn strafbare handelingen kan uitvoeren. Zo zijn bijvoorbeeld DDoS aanvallen, ransomware en andere vormen van malware verspreiding eenvoudig als dienst te bestellen op het internet.

Wat echter minder eenvoudig is voor de cybercrimineel, is anoniem blijven en geen sporen achterlaten. Hier ligt dan ook de kans voor het opsporen van een cybercrimineel. Tijdens de Cybercrime trainingen geven we de deelnemers inzicht in hoe cybercrime werkt, welke sporen een cybercrimineel kan achterlaten en hoe deze sporen gebruikt kunnen worden in een onderzoek.

Cybercrime

Cybercrime, de aangifte

Medewerkers van de Intake & Service afdeling bij de politie zijn het eerste aanspreekpunt bij een aangifte en leggen de fundering voor een opsporingsonderzoek. De training Cybercrime, de aangifte is speciaal gericht op deze medewerkers. Ze leren op een juiste wijze aangifte van cybercrime op te nemen. Het verzamelen van de juiste informatie en het herkennen van de soms vluchtige sporen zijn belangrijk in dit proces. Deze onderwerpen komen dan ook uitgebreid aan bod tijdens de training. Ook wordt er besproken hoe de juiste vertaalslag gemaakt kan worden van cybercrime naar het Wetboek van Strafrecht.

Voor wie is deze training bedoeld?

Deze tweedaagse training is uitermate geschikt voor medewerkers van Intake en Service van de politie.

Wat leert u tijdens de training?

Aan het einde van deze training zijn cursisten op de hoogte van de trends, ontwikkelingen, kansen en bedreigingen rondom cybercrime en digitalisering. Daarnaast zijn ze in staat cybercrime aangiftes op te nemen. Ook hebben ze geleerd veilig een kleine zoekslag te maken op het internet. Verder weten ze hoe ze een beter wachtwoordbeleid voeren en phishing herkennen.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online. Verder is de trainingen modulair opgebouwd waardoor het ook mogelijk is om een maatwerk training samen te stellen met bijpassende casuïstiek.

Leerlijn Cybercrime & Teams

Door de aanzienlijke stijging van cybercrime is de vraag naar gespecialiseerde rechercheurs op dit gebied groot. Om deze vorm van criminaliteit beter te bestrijden, is het belangrijk dat rechercheurs en onderzoekers beschikken over de juiste mix van competenties en vaardigheden.

De leerlijn Cybercrime & Teams bestaat uit drie losse trainingen waarbij het kennisniveau iedere training verder wordt verhoogd en de competenties worden uitgebouwd. Zo worden alle aspecten van het onderzoeken van cybercrime en gedigitaliseerde criminaliteit behandeld.

Deze leerlijn bestaat uit de trainingen:

- Cybercrime Investigations – 4 dagen
- Cybercrime Advanced – 3 dagen
- Cybercrime Professional – 3 dagen

De trainingen zijn opeenvolgend, maar worden los van elkaar gepland. Hierdoor krijgen de deelnemers de gelegenheid tussentijds de lesstof te laten bezinken en te reflecteren. Dit kan door middel van de informatie aanwezig op het e-learning platform en door de kennis opgedaan tijdens de training toe te passen in de praktijk. Daarnaast is het ook mogelijk één of twee trainingen van de leerlijn te volgen wanneer dit toereikend is voor de functie die de cursist bekleedt.

Voor wie is de leerlijn bedoeld?

Deze leerlijn is geschikt voor rechercheurs die zich structureel bezighouden/in aanraking komen met zowel eenvoudige als complexe cybercrime onderzoeken. Denk hierbij aan rechercheurs die in een cybercrime team (gaan) werken. Voor deze leerlijn is geen instapniveau vereist.

Wat leert u tijdens deze leerlijn?

Na het volgen van de Cybercrime trainingen Investigations, Advanced en Professional is de rechercheur in staat eenvoudige en complexe(re) cybercrime processen in kaart te brengen en te onderzoeken. Hierbij heeft hij/zij oog voor mogelijke afbreukrisico's en zijn/haar eigen veiligheid. Ook weet de rechercheur hoe een dossier moet worden opgebouwd en onderbouwd. Voor de verdere inhoud van de trainingen verwijzen wij u naar de individuele trainingen.

Extra informatie

De trainingen in deze leerlijn worden ondersteund door het e-learning platform van DataExpert. Hier kunnen deelnemers kennisnemen van de theorie door middel van tekst en korte video's. Verder kan de training zowel online als klassikaal worden verzorgd.

Cybercrime & Teams 2024 update

Deze 2-daagse training richt zich op personen die reeds succesvol de leerlijn cybercrime hebben voltooid. We concentreren ons niet alleen op de nieuwste trends en ontwikkelingen binnen het domein van cybercriminaliteit, maar reflecteren ook op de vaardigheden en kennis opgedaan tijdens de eerdere Cybercrime & Teams training. De docent beoordeeld de mate waarin de leerdoelstellingen behouden zijn gebleven en welke thema's extra aandacht vereisen. Gedurende deze herzieningssessie zullen we ook een specifieke case doornemen, van aangifte tot de afhandeling ervan, met een focus op het effectief zoeken en juist interpreteren van bewijsmateriaal.

Voor wie is deze training bedoeld?

De wereld van cybercrime ondergaat snelle veranderingen, daarom blijkt een jaarlijkse update gewenst. Deze herzieningssessie is bedoeld voor deelnemers die zich dagelijks bezighouden met cybercrime-onderzoeken of die in het verleden de training Cybercrime & Teams hebben gevolgd.

Extra informatie

De trainingen in deze leerlijn worden ondersteund door het e-learning platform van DataExpert. Hier kunnen deelnemers kennisnemen van de theorie door middel van tekst en korte video's. Verder kan de training zowel online als klassikaal worden verzorgd.

Cybercrime Investigations

Cybercrime en gedigitaliseerde criminaliteit zijn onderwerpen waar iedereen binnen de opsporing mee te maken krijgt. Door de maatschappelijke digitalisering zijn onderzoeken naar cybercrime en gedigitaliseerde criminaliteit de laatste jaren enorm toegenomen. Ook andere opsporingsonderzoeken bevatten een steeds groter cybercomponent. Kennis van de digitale wereld kan daarom van grote meerwaarde zijn voor alle opsporingsonderzoeken.

Voor wie is deze training bedoeld?

Deze training is geschikt voor eenieder binnen de opsporing die zich wil verdiepen in de wereld van cybercrime, waaronder rechercheurs belast met eenvoudige cybercrime onderzoeken en digitale wijkagenten.

Wat leert u tijdens de training?

Aan het eind van deze training hebben de cursisten inzicht gekregen in de huidige trends, ontwikkelingen, kansen en bedreigingen rondom cybercrime en digitalisering. Tijdens de training doorlopen de deelnemers het proces van cybercrime aangifte tot de zaak die uiteindelijk wordt ingestuurd naar Justitie. Hierbij wordt er onder andere aandacht besteed aan de volgende onderwerpen:

- De basiskennis internet- en computertechniek door middel van e-learning.
- De nationale juridische kaders omtrent cybercrime en de bevoegdheden.
- Het voorbereiden en uitvoeren van een zoeking i.v.m. cybercrime.
- Het beperken van afbreukrisico's tijdens een onderzoek.
- Het interpreteren en onderzoeken van veiliggestelde data uit een smartphone.
- Het interpreteren van mailheaders gedurende een onderzoek naar phishing.
- Een kort onderzoek uitvoeren op internet ter verrijking van het eigen onderzoek.
- Het opstellen van een interview/verhoorplan en een rapportage.

Extra informatie

Deze training is onderdeel van de leerlijn Cybercrime & Teams waartoe ook de trainingen Cybercrime Advanced en Professional behoren. De training wordt ondersteund door het e-learning platform van DataExpert. Hier kunnen deelnemers kennisnemen van de theorie door middel van tekst en korte video's. De training wordt in het Nederlands verzorgd en kan zowel klassikaal als online plaatsvinden.

Cybercrime Advanced

De strijd tegen cybercrime vraagt om een gecoördineerde aanpak binnen de opsporing. Tijdens de training Cybercrime Advanced gaan we dieper in op de internet- en computertechniek om kansen binnen een (cyber) onderzoek nog beter te benutten. Waar eenieder binnen de opsporing vroeg of laat in aanraking komt met cybercrime of gedigitaliseerde criminaliteit, zijn er natuurlijk ook de onderzoekers en specialisten die hier dagelijks onderzoek naar doen. De Cybercrime Advanced training biedt deze onderzoekers en specialisten een verbreding van de kennis, competenties en tools om de onderzoeken (nog) efficiënter uit te voeren.

DataExpert

Voor wie is deze training bedoeld?

De training is bedoeld voor eenieder in de opsporing die zich actief bezighoudt met het onderzoeken van cybercrime of gedigitaliseerde criminaliteit. Dit zijn rechercheurs met als taakaccent cybercrime, teamleiders die cybercrime specialisten aansturen en rechercheurs met de intentie om als vraagbaak omtrent cybercrime te fungeren binnen een rechercheteam. Het is wenselijk dat deelnemers aan deze training eerst de training Cybercrime Investigations succesvol hebben afgerond.

Wat leert u tijdens de training?

Na het volgen van de training zijn de cursisten in staat cybercrime onderzoeken uit te voeren naar veiliggestelde data en te adviseren in cybercrime onderzoeken. Hierbij wordt er onder andere aandacht besteed aan de volgende onderwerpen:

- De actuele trends en ontwikkelingen in cybercrime.
- De nationale/Europese bevoegdheden en juridische kaders omtrent cybercrime.
- Het onderzoeken van de front-end van bijvoorbeeld een phishing website of webwinkel.
- Het onderzoeken van complexe mailheaders en DNS-records.
- Het uitlezen, onderzoeken en interpreteren van data van veiliggestelde gegevensdragers.
- Het uitvoeren van basisonderzoek op het darknet.
- Het onderzoeken en in kaart brengen van IoT en connected devices.

Extra informatie

Deze training is onderdeel van de leerlijn Cybercrime & Teams waartoe ook de trainingen Cybercrime Investigations en Professional behoren. De training wordt ondersteund door het e-learning platform van DataExpert. Hier kunnen deelnemers kennisnemen van de theorie door middel van tekst en korte video's. De training wordt in het Nederlands verzorgd en kan zowel klassikaal als online plaatsvinden.

Cybercrime Professional

De stijging van cybercrime is de afgelopen jaren aanzienlijk. Mede hierdoor geven het OM en de politie een hoge prioriteit aan het bestrijden ervan. De politie heeft inmiddels verschillende "cybercrime" teams opgericht, maar ook een "hacking" team en een "darkweb" team. De rechercheurs werkzaam in een cybercrime team krijgen te maken met complexe cybercrime onderzoeken. Deze training staat in het teken van het voorzien van deze rechercheurs van de juiste kennis omtrent complexe cybercrime onderzoeken.

Voor wie is deze training bedoeld?

Deze training is geschikt voor rechercheurs die zich structureel bezighouden/in aanraking komen met zowel eenvoudige als complexe cybercrime onderzoeken. Het is wenselijk dat deelnemers aan deze training eerst de trainingen Cybercrime Investigations en Cybercrime Advanced succesvol hebben afgerond.

Wat leert u tijdens de training?

Na het volgen van deze training zijn de cursisten in staat complexe(re) cybercrime processen in kaart te brengen

en te onderzoeken. Naast het opsporen van cybercriminelen kan het verstoren van een cybercrime proces ook een gewenst resultaat zijn. Tijdens deze training wordt daarom tevens aandacht besteed aan Publiek Private Samenwerking en “out of the box” denken. Hierbij wordt er onder andere aandacht besteed aan de volgende onderwerpen:

- De actuele trends en ontwikkelingen in cybercrime.
- De internationale bevoegdheden en de juridische kaders omtrent cybercrime.
- Het onderzoeken van de back-end van bijvoorbeeld een phishing website of webwinkel.
- Het uitvoeren van een digitaal forensisch onderzoek op een inbeslaggenomen server.
- Het uitvoeren van een basisonderzoek naar een crypto geldspoor met behulp van een ransomware casus.
- Het in kaart brengen en verstoren van een cybercrime proces.
- Het werken met virtualisatie met behulp van tooling zoals Linux Command Line en KALI Linux.

Extra informatie

Deze training is onderdeel van de leerlijn Cybercrime & Teams waartoe ook de trainingen Cybercrime Investigations en Advanced behoren. De training wordt ondersteund door het e-learning platform van DataExpert. Hier kunnen deelnemers kennisnemen van de theorie door middel van tekst en korte video’s. De training wordt in het Nederlands verzorgd en kan zowel klassikaal als online plaatsvinden.

Digitaal Vaardig Rechercheur (DVR)

In de maatwerk opleiding Digitaal Vaardig Rechercheur krijgen cursisten een compleet beeld van alles wat digitaal opsporen en cybercrime behelst. Na de training zijn de deelnemers in staat om passende opsporingsmethoden toe te passen. Ook kunnen ze als tactisch onderzoeker kansen herkennen binnen het digitale domein.

Verder wordt het algemene inzicht omtrent ‘cyber’ en digitaal onderzoek vergroot. De deelnemers weten digitale afbreukrisico’s in te schatten en daar naar te handelen. Tevens zijn ze in staat om telefoondata verantwoord te onderzoeken en de eerste maatregelen op een digitaal plaats delict te nemen.

Voor wie is deze training bedoeld?

Deze training is geschikt voor tactisch rechercheurs werkzaam binnen opsporingsteams verbonden aan high impact crime, thematische opsporing, team grootschalige opsporing, etc.

Wat leert u tijdens de training?

- Het uitvoeren van een eenvoudig dataonderzoek.
- Veel voorkomende onderzoeksprogramma’s te gebruiken.
- Basisbegrippen rondom digitaal onderzoek en cyber.
- Hoe de wereld van cryptocurrency en het darkweb eruitziet.
- Minimaliseren van afbreukrisico’s bij internetonderzoek en onderzoek op locatie.
- De basisbegrippen van interceptie.

DataExpert

- Behandeling van digitale sporen.
- Het verantwoord betreden van een digitale plaats delict.

Extra informatie

De training is een combinatie van e-learning en klassikale training. In overleg kan de training ook online worden verzorgd. Daarnaast kan de training zowel in het Nederlands als Engels worden gegeven.

Notities

Cyber Security

De digitale wereld ontwikkelt zich razendsnel. Deze ontwikkeling gaat niet alleen gepaard met nieuwe kansen, maar ook met bedreigingen. Cybercriminelen, waaronder hackers, hebben helaas steeds minder technische kennis nodig om een land, onderneming of persoon online schade toe te brengen. Het beveiligen van data tegen cybercriminelen door middel van cyber security wordt dan ook steeds belangrijker.

Tijdens onze Cyber Security workshops worden de deelnemers zich meer bewust van de mogelijkheden en de gevaren van cybercrime. Hierdoor kunnen de cursisten na afloop van de trainingen cyberdreigingen beter herkennen, zelf actie ondernemen en de daarbij gepaste maatregelen nemen.

Cyber Security

Cybercrime en Cyber Security Awareness

Ransomware, datalekken en phishing zijn schering en inslag. De vraag is niet of u getroffen wordt, maar wanneer. Een datalek bij een andere organisatie betekent ook niet dat uw organisatie achterover kan leunen. Een belangrijke stap in het voorkomen van slachtofferschap door cybercrime is het bewustmaken van de medewerkers hoe te handelen.

Voor wie is deze training bedoeld?

De workshop Digitale Awareness bestaat uit één dag met daarin drie trainingssessies van ieder twee uur om de verschillende groepen medewerkers binnen een organisatie bewust(er) te maken van cybercrime. Per sessie worden de accenten verlegd, afhankelijk van de functiegroep van de deelnemers.

Wat leert u tijdens de training?

Tijdens iedere trainingssessie wordt er aandacht besteed aan de trends van cybercrime, maar ook aan relevante wetgeving waaronder de AVG. Het doel van de workshop is om de deelnemers weerbaarder te maken, inzicht te geven in hoe te handelen, maar ook ze bewust te maken van ieders verantwoordelijkheid en hoe zich dit verhoudt tot andere onderdelen van de organisatie. Verder is er voldoende ruimte voor interactie; deelnemers kunnen vragen stellen en er wordt gebruik gemaakt van stellingen en/of dilemma's.

De onderwerpen die onder andere aan bod komen in de trainingssessies zijn:

- Cybercrime (actoren, motivatie, doelstellingen).
- Risico's voor de organisatie/medewerker.
- (Praktische) Maatregelen.
- Beleid.
- Relevante wetgeving (AVG en meer).

De intentie is om de individuele medewerker bewust te maken van zijn/haar positie in de verdediging en strijd tegen cybercrime binnen de organisatie.

Extra informatie

Per sessie kunnen er zich maximaal 25 deelnemers aanmelden. Hierbij dient rekening te worden gehouden met homogene groepen qua werkzaamheden. De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

DataExpert

Security Discovery

Als een cyberincident u treft, moet uw organisatie voorbereid zijn om snel en adequaat te handelen. Hiermee kan (financiële) schade aanzienlijk worden beperkt. Maar hoe staat u er nu voor, zowel technisch als procesmatig? Wat is uw baseline? Tijdens deze drie-uur durende workshop neemt een specialist van DataExpert u en uw collega's mee in de wereld van Cyber Security.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor (IT)technische teamleden en management die hun baseline willen bepalen en willen weten waar hun cyberrisico's liggen.

Wat leert u tijdens de training?

- Verloop van cyberaanval.
- Technische en procesmatige maatregelen.
- Werken met security frameworks (bijvoorbeeld NIST, CIS, GDPR, ISO27001).
- Direct te implementeren maatregelen.

Aan de hand van aanvalsmethodiek van cybercriminelen geven we u inzicht in de technieken en processen die u kunt inzetten om 'quick wins' te realiseren. Hierbij beantwoorden we vragen als: Waar staat uw organisatie op dit moment, wat is de benchmark, welke acties heeft u al gedefinieerd (en welke nog niet)? Wat is bedrijfskritisch en voor welke afdeling?

Verder we bespreken wat security frameworks voor mogelijkheden en onmogelijkheden voor uw organisaties bieden en geven we direct pragmatisch advies op het gebied van mens, proces en techniek. Dit resulteert in een gespreksverslag met korte en lange termijn handvatten voor uw organisatie en direct uitvoerbare acties.

Extra informatie

Deze workshop kan in het Nederlands of Engels worden verzorgd. Voor een succesvolle workshop is het van belang dat deze fysiek kan plaatsvinden en wordt de organisatie verzocht om voorafgaand aan de sessie informatie met ons te delen.

Incident Response Readiness

Als een cyberincident u treft, moet uw organisatie voorbereid zijn om snel en adequaat te handelen. Hiermee kan (financiële) schade aanzienlijk worden beperkt. Om uw organisatie voor te bereiden op zo'n situatie, biedt DE-CERT de Incident Response Readiness workshop.

Tijdens deze twee-uur durende workshop neemt een Incident Regievoerder van DataExpert u en uw collega's mee in de wereld van Incident Response.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor alle organisaties die zich willen voorbereiden op een mogelijk cyber incident.

Wat leert u tijdens de training?

- Het verloop van een cyber aanval.
- Wat Incident Response inhoudt.
- Wat een forensisch onderzoek inhoudt en wat het oplevert.
- Alles rondom ransomware betalingen.
- De rol van Politie en de Autoriteit Persoonsgegevens.
- De interne en externe impact van een cybercrisis.
- De korte en lange termijn gevolgen.

Aan de hand van praktijkvoorbeelden geven we u inzicht in de werkwijzen van onze Incident Responders. We tonen hoe een gedegen Incident Response voorbereiding kan bijdragen aan het sneller back-in-business krijgen van uw organisatie. We bespreken hoe wij bij een cyberincident in uw organisatie te werk zouden gaan en gaan ook in op de niet-technische zaken zoals leiderschap, communicatie en risicomanagement. Verder ontvangt u praktische tips om uw organisatie voor te bereiden op een mogelijk incident, handvatten voor te nemen acties rondom inzicht en risico's en we stellen gezamenlijk een incident stappenplan op over hoe u kunt handelen bij een cyberaanval in uw organisatie.

Extra informatie

Deze workshop kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

Digital Forensics

Laptops, mobiele telefoons, de cloud en andere gegevensdragers bevatten onnoemelijk veel informatie. Voor de digitaal rechercheur de uitdaging om op een forensisch correcte manier relevante data hieruit te filteren en kritisch te analyseren zodat het aangetroffen materiaal vervolgens als bewijsmateriaal kan dienen.

Tijdens de Digital Forensics trainingen van DataExpert krijgen cursisten kennis en vaardigheden in het effectief gebruiken van technologie op het gebied van mobile, digital en cloud forensics. Op deze manier worden onderzoeken naar digitale criminaliteit grondiger en analyses sterker.

Digital Forensics

Amped FIVE: Forensic Image and Video Enhancement

Amped is wereldleider op het gebied van beeldbewerking van digitale foto's en video's. Amped FIVE is speciaal ontworpen voor forensische en beveiligingstoepassingen. Tijdens deze training leren cursisten op een eenvoudige, snelle en nauwkeurige wijze werken met deze unieke en complete oplossing. De klassikale training beslaat 4 dagen van 9 tot 5. De online versie beslaat 5 dagen van 9.00 tot 13.00 uur.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor gebruikers die net zijn gestart met het programma Amped FIVE. Dit is de instapcursus voor rechercheurs die zich bezighouden met multimedia onderzoek.

Wat leert u tijdens de training?

Deelnemers aan deze cursus leren de basics van beeld- en video analyse en daarnaast hoe om te gaan met de digitaal multimedia bewijsmateriaal. De cursisten verwerven de juiste kennis en vaardigheden om foto- en videomateriaal op een forensisch correcte manier te verwerken en te analyseren.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Amped FIVE Additions

Tijdens deze opfriscursus leren cursisten de nieuwste filters en functionaliteiten van Amped FIVE en hoe ze data met behulp van deze tool op de juiste wijze kunnen interpreteren. De klassikale training beslaat 3 dagen van 9 tot 5. De online versie beslaat 5 dagen van 9.00 tot 13.00 uur.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor cursisten die de Amped FIVE Basic training reeds hebben gevolgd.

Wat leert u tijdens de training?

De deelnemers leren beeldmateriaal op een forensisch verantwoorde wijze te verwerken en te herstellen. Daarnaast leren de cursisten beeldmateriaal aan te scherpen en te analyseren met behulp van Amped Five software.

Extra informatie

De Additions training is modulair opgebouwd en kan deels op maat worden verzorgd. Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

DataExpert

Amped Authenticate

Amped Authenticate is software voor forensische beeldauthenticatie, sabotagedetectie en camera ballistiek op digitale beelden. Met Authenticate kan de beeldintegriteit, authenticiteit, metadata, bron en geschiedenis achter een afbeelding geanalyseerd worden. Tijdens deze hands-on training verwerven deelnemers de kennis en vaardigheden die nodig zijn om digitale beelden op de juiste manier te analyseren met Amped Authenticate. De klassikale training beslaat 3 dagen van 9 tot 5. De online versie beslaat 5 dagen van 9.00 tot 13.00 uur.

Voor wie is deze training bedoeld?

Dit is een expert level training, bedoeld voor onderzoekers en digitaal rechercheurs die Amped Authenticate willen gebruiken tijdens hun onderzoeken.

Wat leert u tijdens de training?

Deelnemers leren technieken om authenticatieanalyses uit te voeren op digitale beelden in een forensisch wetenschappelijke setting en om die bevindingen samen te vatten en te presenteren in de rechtszaal.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Amped Replay

Amped Replay is een videospeler en converter waarmee een digitaal rechercheur zelf snel en eenvoudig video-bewijsmateriaal kan onderzoeken. Door de gebruiksvriendelijke interface is deze software zowel geschikt voor de ervaren als de beginnend rechercheur. Tijdens deze training verwerven deelnemers de kennis en vaardigheden die nodig zijn om beeld- en videobewijsmateriaal op de juiste manier te onderzoeken en te verwerken met behulp van cases met Amped Replay. De klassikale training beslaat 2 dagen van 9 tot 5. De online versie beslaat 3 dagen van 9.00 tot 13.00 uur.

Voor wie is deze training bedoeld?

Dit is een instapcursus voor opsporingsmedewerkers en first responders.

Wat leert u tijdens de opleiding?

- Hoe u een juridisch proces implementeert voor het gebruik en rapporteren van beeld- en videobewijs in dagelijkse onderzoeken.
- Wat de basisprincipes van beeld- en videoanalyse zijn.
- Hoe u gepatenteerde videobestanden converteert.
- Hoe u basiscorrecties toepast op een beeld.
- Hoe u het bewijsmateriaal voorbereidt voor presentaties met redacties en annotaties.
- Wat de uitdagingen en valkuilen zijn bij het gebruik van digitaal multimedia bewijs in onderzoeken.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Berla iVe Vehicle System Forensics

Berla is leverancier van oplossingen op het gebied van voertuigsystemen. Aan de hand van de aangetroffen voertuigdata kunnen rechercheurs snel en efficiënt vaststellen wat er is gebeurd, waar het is gebeurd en wie er bij betrokken waren.

Tijdens deze vijfdaagse hands-on training leren de cursisten op interactieve wijze om te gaan met voertuigdata aan de hand van het programma iVe. Ze leren werken met deze krachtige software en op efficiënte wijze informatie te vinden over recente bestemmingen, favoriete locaties, gevoerde telefoongesprekken et cetera.

Voor wie is de training bedoeld?

Deze training is bedoeld voor digitaal rechercheurs werkzaam in overheidsdienst of het bedrijfsleven.

Wat leert u tijdens de training?

Na een korte theoretische inleiding zal al snel worden overgegaan naar praktische oefeningen zoals het verwijderen van infotainmentsystemen uit voertuigen en het uitlezen van de data. De deelnemers leren hoe data te kopiëren en te analyseren van diverse infotainmentsystemen zoals Microsoft Sync, MyFord Touch, OnStar, Uconnect en Entune.

Extra informatie

Deze training is in het Engels en wordt klassikaal verzorgd.

Cellebrite Apple Forensics Fundamentals (CAFF)

Deze vierdaagse Apple Mac training is bedoeld voor digitaal rechercheurs die al bekend zijn met forensisch onderzoek op basis van het Windows-platform. Tijdens de Cellebrite Apple Forensic Fundamentals (CAFF) training leren deelnemers onder meer hoe ze Cellebrite Digital Collector en Inspector inzetten voor de analyse van specifieke datapunten binnen besturingssystemen en file system artefacten. Het betreft een praktische training waarbij gewerkt wordt aan de hand van een case.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor digitaal rechercheurs die al ervaring hebben met digitaal onderzoek in het algemeen en hun kennis willen uitbreiden met het onderzoeken van Apple apparaten. Dit is de basiscursus voor alle andere Cellebrite Apple Forensics trainingen.

DataExpert

Wat leert u tijdens de training?

- Verschillende opstartprocedures van Apple apparaten.
- Opstellen van een plan voor succesvolle triage en imaging.
- MacOS structuren en de bijbehorende beperkingen.
- Belangrijkste HFS+ en APFS file system artefacten.
- Impact van veranderingen in de APFS en macOS structuur op forensische analyse.
- Omgang van macOS met property-list (PLIST) data.
- Identificeren van voorkeursinstellingen en systeemvoorkeuren van gebruikers.
- Invloed van datum/tijd en tijdzone op data analyses.
- Herkennen van de verschillende disk images aangetroffen op een macOS.
- Opslaan, bekijken en delen van aangetroffen media files op een macOS en iOS.
- Analyseren van Apple metadata atributen.
- Analyseren van mounted volumes, device connections en netwerkverbindingen in macOS.
- Onderzoeken van artefacten van webbrowsers zoals Safari.
- Interpreteren van aangetroffen log files op macOS- en iOS-apparaten.

Extra informatie

Deze training wordt in het Engels gegeven.

Cellebrite Apple Intermediate Forensics (CAIF)

In deze driedaagse training wordt o.a. dieper ingegaan op het analyseren van macOS- en iOS-apparaten. In de cursus werken de deelnemers aan een case waarbij zij gebruikmaken van de Cellebrite Inspector software.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor digitale rechercheurs met een basiskennis van macOS- en iOS-apparaten die hun kennis willen uitbreiden en een hoger niveau van bekwaamheid willen bereiken. Geadviseerd wordt om eerst de Cellebrite Apple Forensics Fundamentals training te volgen voordat er gestart wordt met deze training.

Wat leert u tijdens de training?

- Analyseren van mounted volumes, device connections en netwerkverbindingen in macOS.
- Interpreteren van aangetroffen log files op macOS- en iOS-apparaten om zo Apple Mail te analyseren inclusief de structuur, e-mail berichten en gerelateerde bestanden.
- Identificeren van bewijs rondom het gebruik van Terminal.
- Herkennen van de GUID Partition Table en het begrijpen van de structuur.
- Begrijpen van de Hierarchical File System (HFS+).
- Onderscheiden en interpreteren van APFS-schijfstructuren van verschillende macOS-versies.
- Creëren, onderzoeken en analyseren van een APFS-schijf.
- Herkennen en begrijpen van de verschillen tussen link files, APFS-clones en APFS-farmlinks in macOS.
- Maken en analyseren van Time Machine back-ups en APFS Snapshots.

Extra informatie

Deze training wordt in het Engels gegeven.

Cellebrite Apple Advanced Forensics (CAAF)

Besturingssystemen laten complexe sporen achter in zowel de toegewezen ruimte als de niet toegewezen vrije ruimte op een datadrager. In deze driedaagse training wordt o.a. ingegaan op de complexere concepten, zoals herstel-punten aangetroffen in een iOS- en macOS-onderzoek. De Cellebrite Apple Advanced Forensics training wordt door een docent geleid die uitgebreide uitleg geeft over de materie, maar er worden ook veel praktische oefeningen gedaan door de deelnemers zelf.

Voor wie is deze training bedoeld?

Deze training is voor gevorderde digitaal rechercheurs met goede kennis van Computer Forensics en uitgebreide kennis van Mac forensisch onderzoek verkregen in b.v. de Cellebrite Apple Intermediate Forensics training.

Wat leert u tijdens de training?

- Onderscheid maken in de omgang met verwijderde APFS en HFS+ bestanden.
- Herstellen van artefacten in zowel toegewezen als niet toegewezen ruimtes.
- Herkennen van hardware en software RAID systemen.
- Begrijpen van geavanceerde iOS-analysepraktijken.
- Gebruiken van logbestanden om de gebruiksgeschiedenis te reconstrueren en tijdlijnen te maken.
- Begrijpen en onderzoeken van Extended Attributes, Spotlight evidence en file sharing artefacten.
- Identificeren en gebruiken van op macOS-opgeslagen wachtwoorden.

Extra informatie

Deze training wordt in het Engels gegeven.

Cellebrite Mobile Forensics Fundamentals (CMFF)

Deze tweedaagse introductietraining is de basis in Mobile Forensics met UFED. Aan de orde komen o.m. Android- en iOS bestandssystemen, communicatienetwerken, extractiemethoden en (NAND) geheugen functies. Verder komt tijdens de training aan bod hoe met digitaal bewijsmateriaal om te gaan en de andere aspecten van het forensische proces.

Voor wie is deze training bedoeld?

De training is bedoeld voor de beginnende digitaal rechercheur. Basiskennis van computersystemen is hierbij een pré.

DataExpert

Wat leert u tijdens de training?

- Verschillende mobiele apparaten en besturingssystemen te vergelijken.
- Verschillende fases in een digitaal forensisch proces te benoemen en te doorlopen.
- Data van het plaats delict en mobiele apparatuur dat als bewijs is aangetroffen te identificeren, verzamelen, onderzoeken en op te slaan.
- Het interpreteren van digitaal bewijs met gebruik van UFED Reader.
- Het analyseren van automatisch gegenereerde rapporten met UFED Touch en 4PC.

Extra informatie

Deze training wordt in het Engels gegeven.

Cellebrite Certified Operator (CCO)

Deze tweedaagse training is bestemd voor rechercheurs die zich bezighouden met het maken van extracties van mobiele apparaten. De CCO training bouwt voort op het concept van de CMFF cursus. Tijdens de training leren de cursisten logische en fysieke extracties te maken met UFED Touch of UFED 4PC. Verder wordt uitgelegd en gedemonstreerd hoe extracties worden ingelezen en geanalyseerd in Physical Analyzer.

Voor wie is deze training bedoeld?

De training is bedoeld voor de rechercheur met enige ervaring in digitaal onderzoek. Het hebben afgerond van de CMFF training is hierbij een pré.

Wat leert u tijdens de training?

- Het installeren en configureren van UFED Touch of UFED 4PC en Physical Analyzer software.
- Data van het plaats delict en mobiele apparatuur dat als bewijs is aangetroffen te identificeren, verzamelen, onderzoeken en op te slaan.
- Met de juiste functionaliteiten van UFED Touch of UFED 4 PC data extracties uitvoeren.
- Met Physical Analyzer dataextracties openen, onderzoeken en rapporteren.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Cellebrite Certified Physical Analyst (CCPA)

Deze driedaagse training richt zich op het analyseren van reeds gemaakte extracties met Physical Analyzer. Tijdens de training worden er geen extracties gemaakt, maar de beschikbare data zal uitvoerig worden onderzocht. Met name de verschillende zoekmethoden komen aan bod.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor technisch onderlegde onderzoekers, analisten en forensisch rechercheurs met ruime ervaring in data analyse. Het hebben afgerond van de CCO training is hierbij een pré.

Wat leert u tijdens de training?

- Geavanceerde forensische mobiele data analyses uitvoeren met UFED Physical Analyzer.
- Authenticatie en validatie van data uit verzameld bewijs met de juiste technieken.
- Verschillende datatypen onderzoeken en resultaten rapporteren met de juiste functionaliteiten van Physical Analyzer.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Cellebrite Evidence Repair Technician – Forensic (CERT-F)

In deze interactieve training leren cursisten hoe ze mobiele telefoons ontmantelen en weer terug in elkaar zetten met als doel een dataextractie op een forensisch juiste manier uit te voeren.

Voor wie is deze training bedoeld?

Deze vijfdaagse training is bedoeld voor (digitaal) rechercheurs en onderzoekers die te maken krijgen met beschadigde mobiele apparaten die reparatie vereisen alvorens data extractie mogelijk is.

Wat leert u tijdens de training?

- Op een juiste wijze belangrijke componenten van mobiele telefoons en USB-drives te vervangen.
- Op een forensisch correcte wijze data veilig te stellen afkomstig van beschadigde mobiele apparaten.
- Onderdelen zoals laadpoorten, lcd-schermen en bepaalde knoppen van een mobiele telefoon te vervangen.
- Het importeren, analyseren en rapporteren van UFDR files in Cellebrite Reader.
- Warmte- en soldeertechnieken.

Aan het einde van deze training leggen de deelnemers een praktijkexamen af waarin ze gebruik maken van UFED technologie. Bij een succesvolle afronding ontvangen de cursisten de Certified Evidence Repair Technician Forensic certificering.

Extra informatie

Deze training wordt in het Engels gegeven en klassikaal verzorgd.

DataExpert

Cellebrite Advanced Smartphone Analysis (CASA)

Deze vijfdaagse training is bestemd voor rechercheurs die zelfstandig smartphones onderzoeken. Tijdens de cursus leren de cursisten hoe ze op efficiënte wijze data kunnen decoderen. Er wordt daarbij gebruik gemaakt van Python scripting en toepassing van datarecovery uit SQLite databases.

Voor wie is deze training bedoeld?

Deze training is geschikt voor digitaal rechercheurs en onderzoekers die ervaring hebben met UFED Physical Analyzer. Het hebben afgerond van de CCPA training is een pré.

Wat leert u tijdens de training?

- Decodering en datarecovery van Smartphones.
- Werken met Python en overige z.g. 3rd party tools.
- Analyse van de gedecodeerde data.
- Validatie van data en rapportage.

Extra informatie

Deze training wordt in het Engels gegeven.

Digitaal opsporen voor de tactische rechercheur

De maatschappij is inmiddels sterk gedigitaliseerd. Mensen zijn 24/7 verbonden met hun netwerk, werk en op vele andere manieren. Binnen de opsporing geeft dit enorme kansen om sporen te vinden en bewijs te leveren. Steeds vaker krijgen tactisch rechercheurs te maken met onderzoeksresultaten uit digitaal forensisch onderzoek. Één van de tools die wordt ingezet bij digitaal onderzoek is AXIOM. Tijdens deze training leren deelnemers te werken met data die gedurende een onderzoek is veiliggesteld met deze tool.

Voor wie is deze training bedoeld?

Deze ééndaagse training is geschikt voor tactisch rechercheurs die in hun dagelijkse werk geconfronteerd worden met allerlei soorten gegevens (data) die zijn geanalyseerd met de tool AXIOM.

Wat leert u tijdens de training?

- Ins en outs rondom AXIOM en het veiligstellen van data door de digitaal rechercheur.
- Lezen van data binnen een AXIOM Portable Case.
- Artefacten (bijv. registry-items).
- Reviewen van verschillende typen documenten en metadata.
- Instellen van filters en tags aanbrengen in relevante data.
- Bekijken van e-mails en analyse van de e-mailheader.
- Analyse van een browser, internethistorie, favorieten en bookmarks.
- Cloud mogelijkheden.
- Timeline onderzoek.

Extra informatie

Voorafgaand aan de training zal de deelnemer middels e-learning basiskennis opdoen van AXIOM. De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

Elastic - Data Analysis with Kibana

Een krachtige zoek- en analyse-engine heeft een even krachtige gebruikersinterface nodig om geavanceerde visualisaties te creëren en diepere analyses uit te voeren. Tijdens deze praktijkgerichte training staat dit centraal. Cursisten leren met behulp van de software Kibana gegevens in Elasticsearch te analyseren.

Voor wie is deze training bedoeld?

Deze training is geschikt voor operationele/zaakanalisten, digitaal rechercheurs en strategische/ tactische analisten die data willen analyseren in Elasticsearch met behulp van Kibana software. De klassikale training beslaat 3 dagen van 9 tot 5. De online versie beslaat 4 dagen van 9.00 tot 15.00 uur.

Wat leert u tijdens de training?

- De kernconcepten van data-analyse met Kibana en Elastic Stack. Denk hierbij aan eenvoudige op aggregatie gebaseerde grafieken maar ook complexe geo-gebaseerde visualisaties en complexe tijdreeksvisualisaties.
- Hoe u zoekslagen maakt met Kibana search.
- Hoe u visualisaties en dashboards maakt voor verschillende datasets.
- Hoe u Kibana beheert.
- Hoe u antwoorden en afwijkingen vindt in uw Elasticsearch-gegevenssets met behulp van Kibana.

Extra informatie

Na het afronden van de training kunt u examen doen om uw certificering te behalen tot Elastic Certified Analyst. Verder wordt deze training in het Engels gegeven en klassikaal verzorgd.

Elastic - Elastic Observability Engineer

Inzicht in datastructuren wordt bereikt wanneer u uw logboeken, statistieken en APM-sporen samenbrengt om een compleet beeld te krijgen van de gezondheid en activiteit van uw infrastructuur. Deze training biedt cursisten een sterke basis voor het gebruik van de Elastic Stack. Op deze manier leren ze een uniforme observatie te implementeren met een single-stack oplossing.

Voor wie is deze training bedoeld?

Deze training is geschikt voor operationele/zaakanalisten, digitaal rechercheurs en strategische/ tactische analisten die inzicht willen scheppen in hun IT infrastructuur. De klassikale training beslaat 3 dagen van 9 tot 5. De online versie beslaat 4 dagen van 9.00 tot 15.00 uur.

DataExpert

Wat leert u tijdens de training?

- Hoe u logs, metrics en APM-data verzamelt en deze vervolgens naar één datastore verzendt: Elasticsearch.
- Hoe u uniforme observatiegegevens actiegericht maakt door middel van machine learning en alarmering.
- Hoe gegevens makkelijker over verschillende databronnen kunnen worden gecorreleerd.
- Hoe u uw waarneembaarheidsgegevens visualiseert via de intuïtieve gebruikersinterface Kibana.

Extra informatie

Na het afronden van de training kunt u examen doen om uw certificering te behalen tot Elastic Certified Observability Engineer. Verder wordt deze training in het Engels gegeven en klassikaal verzorgd.

Elastic - Elasticsearch Engineer

Tijdens deze hands-on training leren de cursisten de basisprincipes om aan de slag te gaan met Elasticsearch en Elastic Stack. Daarna wordt er dieper ingegaan op diverse onderwerpen zoals data modellering, data management, data verwerking, cluster management, het ontwikkelen van zoekapplicaties en shards.

Voor wie is deze training bedoeld?

Deze training is geschikt voor operationele/zaakanalisten, digitaal rechercheurs en strategische/ tactische analisten voor zowel beginners als ervaren gebruikers. De klassikale training beslaat 3 dagen van 9 tot 5. De online versie beslaat 4 dagen van 9.00 tot 15.00 uur.

Wat leert u tijdens de training?

- Hoe Elasticsearch en de onderdelen van Elastic Stack samenwerken.
- Waar en wanneer u welke zoektaal moet gebruiken.
- Wat de verschillende manieren zijn om data te importeren en te verwerken.
- Hoe u complexe query's bouwt en de zoekresultaten hieruit verwerkt.
- Hoe u uw clusters op- en afschaalt.
- Hoe u indices in grote en meerdere clusters beheert.
- De ins en outs rondom data & cluster management.
- Aanbevelingen voor probleemoplossingen.
- Hoe u uw eigen aangepaste zoekapplicaties bouwt die Elasticsearch op de achtergrond gebruikt.

Extra informatie

Na het afronden van de training kunt u examen doen om uw certificering te behalen tot Elastic Certified Engineer. Verder wordt deze training in het Engels gegeven en klassikaal verzorgd.

Elastic - Threat Hunting with Kibana

Tijdens deze training leren cursisten middels opdrachten hoe ze bedreigingen opsporen en hoe dit verschilt met

andere beveiligingsanalyse processen. Vervolgens leren ze Elastic Stack en de daarbij behorende krachtige tools in te zetten ter ondersteuning van dit proces.

Voor wie is deze training bedoeld?

Deze training is geschikt voor beveiligingsanalisten die geïnteresseerd zijn in het gebruik van Kibana met als doel onderzoek naar mogelijke bedreigingen voor hun gegevens en systemen. De klassikale training beslaat 3 dagen van 9 tot 5. De online versie beslaat 4 dagen van 9.00 tot 15.00 uur.

Wat leert u tijdens de training?

- De essentiële Kibana functionaliteiten voor het analyseren van security data.
- Hoe netwerk en host databronnen verrijkt kunnen worden.
- De filosofie, workflow, modellen en technieken die toegepast kunnen worden in de jacht op (cyber)dreigingen.
- Hoe Threat Hunting helpt om de effectiviteit van het Security Operations Center te verbeteren.

Extra informatie

Deze training wordt in het Engels gegeven en klassikaal verzorgd.

Elastic - Networking Security Monitoring Cyber Operator

Tijdens deze vijfdaagse training leren de deelnemers werken met een suite van cybersecurity tools. Hoewel de training over open source security tools gaat, is de Networking Security Monitoring Cyber Operator training geen tool training. Het doel van de training is om Cybersecurity Operators cyberdreigingen te leren detecteren en opsporen met behulp van Elastic Stack en tools zoals Zeek en Suricata. Ter afsluiting van de training werken de deelnemers aan een case met meerdere scenario's, waarbij ze de geleerde vaardigheden inzetten om de 'vijand' te vinden in het netwerkverkeer.

Voor wie is deze training bedoeld?

Deze training is geschikt voor Cybersecurity Operators die gegevens moeten analyseren om slechte actoren in hun netwerk op te sporen als onderdeel van een machine-assisted, human-driven aanpak. Geadviseerd wordt deze training enkel te volgen als u bekend bent met Linux, netwerken en netwerk security concepten.

Wat leert u tijdens de training?

- Basisprincipes van Packet analyse
- Inbraakdetectiesystemen (IDS) met Suricata
- Netwerk Metadata Analyse met Zeek
- Kibana UI voor Security
- Threat hunting Capstone

Extra informatie

Deze training wordt in het Engels gegeven.

Elastic - Network Security Monitoring Engineer

Deze tiendaagse training is gericht op de inzet van Elastic Stack in een security context. Hierbij wordt ingezoomd op de implementatie van de verschillende onderdelen van de Elastic Stack (Elasticsearch, Kibana, Beats en Logstash) en het optimaliseren van de prestatie van deze onderdelen.
Tijdens de training leren de deelnemers alles over de Elastic Stack en zijn kerncomponenten en bouwen ze met deze kennis Netwerk Security Monitoring (NSM) sensoren in verschillende configuraties. Aan het eind van de training zijn de deelnemers in staat de Elastic Stack zo op te bouwen dat ze gegevensbronnen in hun netwerk en systemen kunnen analyseren. Dit met als doel een completer security beeld te creëren.

Voor wie is deze training bedoeld?

Deze training is geschikt voor Security Engineers die verantwoordelijk zijn voor het instaleren, gebruiken en onderhouden van de Elastic Stack en network monitoring platforms.

Wat leert u tijdens de training?

- Ansible
- Zeek installeren, gebruiken, onderhouden en optimaliseren
- Kafka installeren, gebruiken en onderhouden
- Passieve operations en tapping
- CAPES instaleren, gebruiken en onderhouden
- Elastic Stack installeren, gebruiken en onderhouden
- Suricata rule management en tuning
- Sensor troubleshooting
- Engigneer capstone event

Extra informatie

Deze training wordt in het Engels gegeven.

EnCase DF120

EnCase biedt geavanceerde opties voor het onderzoeken van computerdata. Tijdens deze vierdaagse praktijkgerichte training met praktische voorbeeldencases maakt u kennis met de functionaliteiten van deze software.

Voor wie is deze training bedoeld?

Deze vierdaagse training is bedoeld voor digitaal rechercheurs en IT-security deskundigen. De training is geschikt voor rechercheurs die nog geen of weinig ervaring hebben op het gebied van digitaal forensisch onderzoek.

Wat leert u tijdens de training?

- Wat digitaal bewijsmateriaal is en hoe een computer werkt.

- Een overzicht van de EnCase Computer Forensic methodiek.
- Inzicht in de opbouw van Fat en NTFS bestandssystemen.
- Hoe een zaak te creëren.
- Het 'previewen' en 'acquiren' van datadragers.
- Hoe basis 'keyword searches' uit te voeren.
- Hoe digitale footprints te analyseren en bestanden te bekijken.
- Hoe verdachte data te 'restoren'.
- Hoe de resultaten van het onderzoek op te slaan.
- Hoe bewijsmateriaal voor te bereiden en te presenteren in een rechtszaak.
- Hoe bewijsmateriaal te verifiëren.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

EnCase DF210

Deze praktijkgerichte vierdaagse training is bedoeld voor ervaren computergebruikers, die bovendien al enige ervaring hebben met EnCase. Deze training gaat verder waar de EnCase DF120 training ophoudt. De training stelt de digitaal rechercheur in staat om de unieke features van EnCase optimaal te benutten.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor ervaren digitaal rechercheurs en IT-security deskundigen die de EnCase DF120 training hebben afgerond.

Wat leert u tijdens de training?

- Hoe 'logical evidence-files' aan te maken en te gebruiken.
- Hoe verwijderde partities en mappen terug te vinden.
- Hoe geavanceerde zoekopdrachten uit te voeren met behulp van GREP.
- Hoe het Windows Register werkt.
- Hoe om te gaan met samengestelde bestanden.
- Hoe bestanden, directories en de complete inhoud van een schijf te exporteren.
- Hoe te werken met hash-libraries en bestandsidentificatie.
- Hoe Windows onderdelen zoals links, gebruikersfolders en de prullenbak te identificeren binnen EnCase.
- Hoe geprinte pagina's terug te halen.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

DataExpert

EnCase DF220

Deze vierdaagse hands-on training biedt praktische demonstraties en praktijkcases voor een beter begrip van de EnCase Forensic Versie 8 methodologie. Deze training is geen vervanging van de EnCase DF120 & EnCase DF210 trainingen.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor ervaren digitaal rechercheurs die de stap willen maken naar EnCase versie 8. Bijvoorbeeld EnCase versie 6 gebruikers die de EnCase DF210 hebben gevolgd of gebruikers met een ENCE certificering. Ook kan deze training worden toegepast als een opfristraining voor gebruikers van versie 7.

Wat leert u tijdens de training?

- De structurele verschillen tussen EnCase versie 8 en eerdere versies.
- De werking van de modules.
- De nieuwe bestandsstructuur van de 'evidence files' en de transitie vanuit voorgaande versies.
- De nieuwe zoekfunctie.
- Hoe de externe viewing tools te gebruiken.
- Hoe hash analyses uit te voeren.
- Het creëren van rapporten met behulp van de nieuwe templates.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

EnCase DF320

Deze vierdaagse training gaat dieper in op de stof die is behandeld in de EnCase DF210 training en legt de nadruk op het onderzoek van besturingssystemen.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor ervaren digitaal rechercheurs en IT-security deskundigen die de EnCase DF210 hebben afgerond. Basiskennis van Computer Forensics is vereist.

Wat leert u tijdens de training?

- De werking van Windows NT-file Systemen (NTFS).
- Data recovery van NTFS.
- Onderzoek van Windows Registerbestanden.
- Analyse en recovery van de Windows event log files.
- Hard-end Software RAID technologie, acquisitie en onderzoek.
- De principes van Encrypted Data Recovery.
- Begrip van en onderzoek naar Windows BitLocker schijven.

- Linux en UNIX besturingssystemen en bestandsinformatie.
- Linux partitie herstel.
- Forensisch onderzoek van Macintosh computers.
- Het Macintosh besturingssysteem.
- Verdieping van de EnCase computer forensic methodiek.
- Introductie EnScript programmering.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

EnCase DF410-NTFS

In deze vierdaagse training leren de cursisten om te gaan met de technische uitdagingen van het Windows NTFS bestandssysteem en hoe ze de Master File Table aan een diepgaande analyse kunnen onderwerpen. Het betreft een intensieve, praktijkgerichte training met praktische voorbeeldcases.

Voor wie is deze training bedoeld?

De hands-on training is bedoeld voor ervaren digitaal rechercheurs, netwerkbeheerders en de IT-security beheerders die meer inzicht willen krijgen in NTFS en Windows netwerken in relatie tot cybercrime. De deelnemers aan deze training worden geacht bekend te zijn met EnCase. Bovendien dienen ze ruime ervaring te hebben opgedaan op het gebied van computeronderzoek.

Wat leert u tijdens de training?

- De Master File Table (MFT) grondig te analyseren.
- Het NTFS bestandssysteem te doorgronden.
- Windows artefacts te onderzoeken en hun bewijswaarde in te schatten.
- Gewiste NTFS partities terug te vinden.
- Register-informatie te begrijpen zoals de NTUSER.DAT en de SAM-file.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

EnCase DFIR350

Deze vierdaagse training stelt de digitaal rechercheur in staat om bewijsmateriaal aangetroffen op de computer van een verdachte of slachtoffer te interpreteren met behulp van EnCase en gaat onder meer in op de werking van Bit- Torrent P2P netwerken, de werking van Trojan virussen en de werking van de verschillende soorten e-mail clients.

DataExpert

Voor wie is deze training bedoeld?

Deze praktijkgerichte training is bedoeld voor ervaren computergebruikers (digitaal rechercheurs en IT-security deskundigen), die bovendien al enige ervaring hebben met EnCase.

Wat leert u tijdens de training?

- Achtergronden van PTP en BitTorrent.
- De werking van BitTorrent en het BitTorrent protocol.
- De werking van het Gnutella P2P netwerk.
- De werking van de programma's LimeWire en Bearshare.
- De achtergrond en werking van Trojan Virussen.
- Het gebruik van VFS en PDE t.b.v. identificatie en analyse van Trojan's.
- Hoe Keyloggers te detecteren en analyseren.
- De werking en het gebruik van Windows LIVE messenger.
- De werking van Internet History en WebCache.
- Doel, inhoud en het indexeren van internet cookie bestanden.
- Het reconstrueren van webpagina's.
- De opbouw en het analyse van Outlook PST bestanden.
- Het gebruik van Mozilla FireFox.
- Lotus Notes analyse met EnCase.

Extra informatie

Deze training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Forensic Toolkit 101

Als forensisch specialist op een grondige en effectieve manier computeronderzoeken uitvoeren? Tijdens de vier-daagse Forensic Toolkit 101 training maken cursisten kennis met de belangrijkste functionaliteiten en processen van Forensic Toolkit.

Voor wie is deze training bedoeld?

De Forensic Toolkit 101 training is bedoeld voor de digitaal rechercheur/onderzoeker. FTK wordt vooral ingezet door forensisch specialisten en fraudeonderzoekers.

Wat leert u tijdens de training?

- Een FTK case maken en beheren.
- Werken met de FTK Interface.
- De zoekmogelijkheden.
- De filteropties.
- Hoe het Manage Menu werkt.
- Items te exporteren in FTK.

- De Know File Filter (KFF) te installeren en toe te passen.
- Een Disk Level Analysis uit te voeren.
- Te werken met de FTK Python Scripter.
- Data te visualiseren in FTK.
- Rapportages te maken.

Extra informatie

Deze training is in het Engels en kan zowel klassikaal als online worden verzorgd.

Forensic Toolkit 201

Deze vierdaagse Forensic Toolkit 201 training gaat net iets verder dan de Forensic Toolkit 101 training. De FTK 201 training gaat dieper in op de analyse van forensische artefacten met FTK. Ook komt de forensische tool QView van Exterro aan bod.

Voor wie is deze training bedoeld?

De Forensic Toolkit 201 training is geschikt voor digitaal rechercheurs/onderzoekers. Het is aan te raden om eerst de Forensic Toolkit 101 training te volgen.

Wat leert u tijdens de training?

- Welke algemene data structuren er zijn.
- Grafische afbeeldingen en video's te analyseren.
- Het Windows register te analyseren.
- Windows event logs te analyseren.
- Het besturingssysteem van Windows te analyseren.
- Apple MacOS te analyseren.
- Internet browsers te analyseren.
- Cloud-data te interpreteren.
- Werken met QView.

Extra informatie

Deze training is in het Engels en kan zowel klassikaal als online worden verzorgd.

Griffeye Analyze DI Certification

Hoewel meer digitale beelden potentieel ook meer digitaal bewijs met zich meebrengen, is het bijna onmogelijk om zonder de juiste tools waardevolle informatie te achterhalen. Analyze DI Pro van Griffeye kan digitaal forensisch rechercheurs hierin uitstekend ondersteunen. Tijdens deze training komen de belangrijkste functionaliteiten van de tool Analyze DI Pro aan bod.

DataExpert

Voor wie is deze training bedoeld?

Deze vierdaagse training is speciaal voor digitaal forensische teams die zich specifiek bezighouden met z.g. CSAM zaken, dit staat voor Child Sexual Abuse Material.

Wat leert u tijdens de training?

- Over welke features Analyse DI Pro beschikt. Denk hierbij aan functionaliteiten als: het groeperen en doorzoeken van metadata, gezichtsherkenning en afbeelding en video hashing
- Hoe u de tooling kunt inzetten tijdens uw onderzoek.

Extra informatie

Na het succesvol afronden van deze training ontvangen de cursisten het Griffeye Analyze DI Pro certificaat. Verder is deze training is in het Engels en kan zowel klassikaal als online worden verzorgd.

Hansken Advanced training

Hansken is een forensisch data analyse platform dat binnen de Nederlandse opsporingswereld veel wordt ingezet bij strafrechtelijk onderzoek. Het platform ondersteunt analisten en digitaal rechercheurs bij het verkrijgen van toegang tot digitaal bewijsmateriaal, het snel doorzoeken en creëren van inzicht in de aangetroffen data en het in kaart brengen van mogelijke sporen.
Tijdens de hands-on Hansken Advanced training leren digitaal rechercheurs en analisten te werken met de geavanceerde functionaliteiten van Hansken. Dit doen ze aan de hand van een case met voorbeelden uit de praktijk. De focus van de training ligt op de technische gebruikers interface (Hansken Expert UI).

Voor wie is deze training bedoeld?

Deze driedaagse training is geschikt voor analisten en digitaal forensische experts die hun kennis rondom Hansken willen uitbreiden met de meer geavanceerde functionaliteiten. Aanbevolen wordt dat de deelnemers van deze training de Hansken Intermediate training hebben afgerond of al geruime ervaring hebben opgedaan met Hansken tijdens hun werk.

Wat leert u tijdens de training?

- Hoe Hansken sporen uit digitaal bewijsmateriaal haalt
- Geïdentificeerde sporen uit te diepen en te interpreteren
- Complexe zoekopdrachten en geavanceerde queries uit te voeren met het trace model en de query taal
- Bewijsmateriaal (chain of evidence) te verwerken en het proces (chain of custody) te registreren
- Aanwezige tools en statistieken
- Samenwerken met de case operator
- Visualisatiemogelijkheden
- Rapportagemogelijkheden
- Begin van scripting en extractie plug-ins

Overige informatie

Deze training wordt klassikaal gegeven en kan zowel in het Nederlands of Engels worden verzorgd. Gezien het hands-on karakter van de training, krijgen deelnemers toegang tot de Hansken oefenomgeving.

Incident Response in the Microsoft Cloud

In deze tweedaagse hands-on training leert u alles wat u moet weten over forensics en incident response in Microsoft Cloud omgevingen. De training behelst zowel Microsoft Azure als Microsoft 365, u krijgt hands-on ervaring met het onderzoeken van aanvallen en het analyseren van de verschillende log-bronnen die beschikbaar zijn in de cloud. Alles wat u leert is gebaseerd op daadwerkelijke bedreigingen en aanvallen die hebben plaatsgevonden in Microsoft omgevingen. De instructeur heeft zelf ruime praktijkervaring met het uitvoeren van forensics en incident response werkzaamheden in de cloud, deze unieke kennis is niet beschikbaar in documentatie op de Microsoft website.

Vereiste voorkennis

De vereiste voorkennis wordt beschikbaar gesteld via On Demand video's opgenomen door de instructeur en moet bekeken worden voordat de cursus start. De videos gaan over de volgende onderwerpen:

- Azure platform basiskennis waaronder hierarchy van de cloud en Microsoft terminologie
- Azure Active Directory/Entra ID componenten waaronder gebruikers, groepen en service principals
- Audit logging in een Microsoft Azure omgeving

Na het afronden van deze cursus heeft u voldoende kennis zodat u voldoende vertrouwen heeft om zelfstandig een incident response onderzoek in de cloud te kunnen onderzoeken. Het unieke van de training is de praktische skills en ervaring die u zult opdoen door middel van twee volledig uitgewerkte aanval scenario's die u gaat onderzoeken in een Capture-The-Flag (CTF) competitie.

Magnet Forensic Fundamentals (AX100)

Tijdens deze Forensic Fundamentals (AX100) training leren de cursisten de basisvaardigheden voor het uitvoeren van digitaal forensisch onderzoek. Zo komen onder meer de belangrijkste terminologie en de werkprocedures aan bod, maar ook welke type gegevensdragers er zijn en waar de rechercheur met het veiligstellen van bewijsmateriaal rekening mee dienen te houden.

Voor wie is deze training bedoeld?

Deze vierdaagse training is ontworpen voor startende digitaal rechercheurs en onderzoekers die nog niet bekend zijn met de basisprincipes van Digital Forensics.

Wat leert u tijdens de training?

- Wat Magnet AXIOM is.

- Hoe digitaal bewijsmateriaal wordt verzameld en bewaard. Denk hierbij aan de procedures en kaders waarmee de onderzoeker te maken krijgt.
- Schijfgeometrie zoals het definiëren en verwoorden van bepaalde onderdelen van harde schijven en soortgelijke media en welke basiscomponenten deze bevatten, hoe de capaciteit van een schijf berekend wordt en wat het verschil is tussen CHS- en LBA-sectornummering.
- De basisprincipes rondom gegevensopslag (bits, bytes en hex). Hieronder valt onder andere de bijbehorende getallenstelsels en hoe het basisproces werkt van het indrukken van een toets tot de opslag op een harde schijf.
- Alles over partitioneren, formatteren en bestandssystemen zoals de verschillen, de structureren en de daarbij behorende processen.
- Wat een opstartproces en drive letter assigments inhouden en hoe het werkt.
- Wat de principes zijn van gegevensopslag en hoe sectoren op een gegevensdrager worden beïnvloed bij het opslaan, verplaatsen en verwijderen van bestanden.
- Welke informatie het Windows Register bevat en waar de meest voorkomende artefacten zich bevinden.
- Hoe images kunnen worden gemaakt van computer media en mobiele apparaten en hoe Magnet AXIOM daarin kan ondersteunen.
- Hoe inzicht verkregen kan worden in mobiele apparaten van onder meer iPhone en Android en hoe met behulp van rooting en jailbreaking toegang verkregen kan worden tot verdachte toestellen.

Extra informatie

Deze training is modulair opgebouwd. Bij elke module wordt er gebruik gemaakt van scenario's en hands-on oefeningen om de leerdoelen te versterken. Verder wordt de training in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Magnet AXIOM Examinations (AX200)

In deze hands-on cursus leert de cursist op interactieve wijze hoe om te gaan met digitaal bewijsmateriaal dat wordt aangetroffen op computers en mobiele telefoons. De focus ligt daarbij op de sporen die worden aangetroffen na internetgebruik, gebruik van social media en apps op mobiele apparaten. Na de installatie van AXIOM gaan de cursisten aan de gang met het zoeken en analyseren van de data, waarna de bevindingen in een rapport worden vastgelegd.

Voor wie is deze training bedoeld?

Deze vierdaagse training is ontworpen voor digitaal rechercheurs van opsporingsdiensten uit de forensics community zoals politie, defensie, special taskforces maar ook particuliere onderzoeksinstanties. De cursus is geschikt voor zowel de beginnend digitaal rechercheur alsook rechercheurs/onderzoekers die AXIOM al een tijdje gebruiken, maar de training nog niet hebben doorlopen.

Wat leert u tijdens de training?

Na afloop van de training zijn de deelnemers in staat om:

- Magnet AXIOM te configureren.
- Het belangrijkste bewijs (beeldmateriaal) uit de computer en van de smartphones te halen.
- De meest relevante informatie terug te vinden.
- Bewijsmateriaal diepgaander te verkennen.
- De analyse activiteiten te vereenvoudigen en het intuïtief koppelen van feiten en gegevens.
- De belangrijkste artefacten voorbereiden voor samenwerking met andere stakeholders.

Extra informatie

Elke module maakt gebruik van een uitgebreide basis van scenario's en hands-on oefeningen om de leerdoelen te versterken en verdere inzichten te geven aan de deelnemer in de functionaliteit van Magnet AXIOM en de toepassing ervan binnen de forensische workflow. Verder wordt de training in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Magnet AXIOM Advanced Computer Forensics (AX250)

Dit is het vervolg op de AX200 training. In deze hands-on cursus leert de cursist op interactieve wijze hoe om te gaan met digitaal bewijsmateriaal dat wordt aangetroffen op computers. De focus ligt daarbij op de sporen die worden aangetroffen na internetgebruik, gebruik van social media en apps. In deze cursus worden de volgende onderwerpen besproken: geavanceerde zoekmethoden in het RAM-geheugen, encryptie, het decrypten van Windows wachtwoorden en het zoeken naar ontbrekende informatie in cachebestanden.

Voor wie is deze training bedoeld?

Deze vierdaagse training is ontworpen voor digitaal rechercheurs van opsporingsdiensten uit de forensics community zoals politie, defensie, special taskforces maar ook particuliere onderzoeksinstanties. De cursus is geschikt voor de gevorderde digitaal rechercheur, alsook degenen die de AX200 training al hebben gevolgd.

Wat leert u tijdens de training?

Na afloop van de training zijn de deelnemers in staat om:

- Magnet AXIOM te configureren.
- De werking van Windows 10 en de forensische implicaties te doorgronden.
- Registerlocaties te gebruiken en volume serienummers te traceren.
- Te filteren en zoeken naar relevante artefacten.
- App data nader te onderzoeken.
- Prefetch files nader te onderzoeken.
- Het gebruik van een encrypted container vast te stellen.
- iOS backups te onderzoeken en gebruik te maken van de AXIOM Wordlist Generator.
- Cloud data te herkennen en een Gmail account nader te onderzoeken.

Extra informatie

Elke module maakt gebruik van een uitgebreide basis van scenario's en hands-on oefeningen om de leerdoelen

te versterken en verdere inzichten te geven aan de deelnemer in de functionaliteit van Magnet AXIOM en de toepassing ervan binnen de forensische workflow. Verder wordt de training in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Magnet AXIOM Advanced Mobile Forensics (AX300)

Dit is het vervolg op de AX200 training. In deze hands-on cursus leert de cursist op interactieve wijze hoe om te gaan met digitaal bewijsmateriaal dat wordt aangetroffen op mobiele telefoons. De focus ligt daarbij op de sporen die worden aangetroffen na internetgebruik, gebruik van social media en apps op mobiele apparaten. Tijdens deze training worden de volgende onderwerpen besproken: geavanceerde technieken zoals Chip-off, JTAG en ISP en de werking van iOS en Android besturingssystemen.

Voor wie is deze training bedoeld?

Deze vierdaagse training is ontworpen voor digitaal rechercheurs van opsporingsdiensten uit de forensics community zoals politie, defensie, special taskforces maar ook particuliere onderzoeksinstanties. De cursus is geschikt voor de gevorderde digitaal rechercheur, alsook degenen die de AXIOM AX200 training al hebben afgerond.

Wat leert u tijdens de training?

Na afloop van de training zijn de deelnemers in staat om:

- Magnet AXIOM te configureren.
- De verschillende acquisitiemethodes zoals Chip-off, JTAG en ISP te onderscheiden.
- Het iOS besturingssysteem te doorgronden en hoe Apple apparaten te imagen.
- Het Android besturingssysteem te doorgronden en hoe Android apparaten te imagen.
- Het Media Transfer Protocol (MTP) toe te passen.
- De Dynamic App Finder te gebruiken.
- Het gebruik van een encrypted container vast te stellen.
- XML artifacten te creëren en data van SQLite databases te carven.

Extra informatie

Elke module maakt gebruik van een uitgebreide basis van scenario's en hands-on oefeningen, om de leerdoelen te versterken en verdere inzichten te geven aan de deelnemer in de functionaliteit van Magnet AXIOM en de toepassing ervan binnen de forensische workflow. De training in het Engels gegeven en kan deze zowel klassikaal als online worden verzorgd.

Magnet GK200 GRAYKEY Examinations (AX301)

In deze hands-on cursus leert de cursist op interactieve wijze hoe om te gaan met digitaal bewijsmateriaal dat wordt aangetroffen op iOS apparaten in combinatie met GRAYKEY. Tijdens deze training wordt het volgende onderwerp besproken: AXIOM in combinatie met de GRAYKEY unit.

Voor wie is deze training bedoeld?

Deze vierdaagse training is ontworpen voor digitaal rechercheurs van opsporingsdiensten uit de forensics community zoals politie, defensie en special taskforces. De cursus is geschikt voor de gevorderde digitaal rechercheur, alsook degenen die AXIOM al een tijdje gebruiken maar de training nog niet hebben doorlopen. Alleen voor overheidsinstanties na acceptatie van Grayshift!

Wat leert u tijdens de training?

- Magnet AXIOM te configureren.
- De GRAYKEY unit te gebruiken in combinatie met AXIOM.
- Verschillende data-extractie types met elkaar te vergelijken.
- Het iOS besturingssysteem en de Apple beveiliging te doorgronden.
- De Dynamic App Finder en andere functies zoals 'Search for Custom Files by type' te gebruiken.
- Aangetroffen artefacten nader te onderzoeken.

Extra informatie

Elke module maakt gebruik van een uitgebreide basis van scenario's en hands-on oefeningen om de leerdoelen te versterken en verdere inzichten te geven aan de deelnemers in de functionaliteit van Magnet AXIOM en GRAYKEY en de toepassing ervan binnen de forensische workflow. Verder wordt de training in het Engels gegeven en klassikaal verzorgd.

Magnet AXIOM Incident Response Examinations (AX310)

Tijdens de AXIOM Incident Response Examinations (AX310) training leren cursisten aan de hand van een praktijkgerichte case hoe ze een digitaal forensisch onderzoek uitvoeren bij een malware incident. Hierbij maken ze gebruik van Magnet AXIOM en de daarbij horende Incident Response Toolkit.

Voor wie is deze training bedoeld?

Deze vierdaagse training is bedoeld voor digitaal rechercheurs en onderzoekers die vertrouwd zijn met de beginselen van digitaal forensisch onderzoek en die hun kennis willen uitbreiden met geavanceerde forensische- en incident response technieken. Het is wenselijk dat cursisten eerst de Magnet Examinations (AX200) training hebben afgerond.

Wat leert u tijdens de training?

- Over welke functionaliteiten Magnet AXIOM beschikt.
- Wat malware is, welke sporen het achterlaat, hoe het zich gedraagt en hoe het gestopt kan worden.
- Hoe malware via netwerkverkeer kan binnendringen en zich kan verplaatsen en hoe netwerkverkeer kan worden vastgelegd, gefilterd en geanalyseerd tijdens een forensisch onderzoek naar malware.
- Hoe WireShark werkt.
- Hoe aan de hand van de Incident Response Toolkit vluchtige data van een computer kan worden verzameld en output kan worden gecreëerd met behulp van AXIOM om zo de malware te lokaliseren.

DataExpert

- Hoe het RAM geheugen kan worden geanalyseerd van een computer die betrokken is bij een malware incident en hoe in kaart kan worden gebracht welke programma's er op dat moment draaiden en vanaf welke locatie.
- Hoe PCAP bestanden vanuit het RAM geheugen kunnen worden verwerkt ter ondersteuning van een forensisch onderzoek.
- Hoe een statische analyse van malware kan worden uitgevoerd met behulp van een virtual machine.
- Hoe een dynamische analyse van malware kan worden gemaakt.
- Hoe een rapportage van een malware onderzoek gemaakt kan worden met behulp van de artefact-first aanpak van AXIOM.
- Hoe alle losse elementen van een onderzoek geëxtraheerd en met elkaar gecorreleerd kunnen worden.

Extra informatie

Deze training is modulair opgebouwd. Bij elke module wordt er gebruik gemaakt van scenario's en hands-on oefeningen om de leerdoelen te versterken. Verder wordt de training in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Magnet AXIOM Internet and Cloud Investigations (AX320)

Dit is een expert training. Het wordt sterk aanbevolen om eerst de AX200 training te volgen. In deze hands-on cursus leert de cursist op interactieve wijze hoe om te gaan met digitale sporen die worden aangetroffen op het internet en in de cloud. De focus ligt daarbij op de sporen die worden aangetroffen na internetgebruik, gebruik van social media en apps. In deze cursus wordt vooral aandacht besteed aan acquisitie en onderzoek van cloud-data met behulp van AXIOM en open-source tools en technieken.

Voor wie is deze training bedoeld?

Deze vierdaagse training is ontworpen voor digitaal rechercheurs van opsporingsdiensten uit de forensics community zoals politie, defensie, special taskforces maar ook particuliere onderzoeksinstanties. De cursus is geschikt voor de gevorderde digitaal rechercheur die zijn kennis wil uitbreiden op het gebied van cloudonderzoek en social media forensics.

Wat leert u tijdens de training?

Onderwerpen die tijdens de training aan de orde komen, zijn:

- Onderzoeksmethoden naar cloud-data.
- De cloud aspecten van Apple, Google, Microsoft, Twitter, Facebook, Instagram, Dropbox, Box en e-mail.
- Herhaling van het geleerde incl. afsluitende oefening.

Extra informatie

Elke module maakt gebruik van een uitgebreide basis van scenario's en hands-on oefeningen om de leerdoelen te versterken en verdere inzichten te geven aan de deelnemer in de functionaliteit van Magnet AXIOM en de toepassing ervan binnen de forensische workflow. Verder wordt de training in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Magnet AXIOM macOS Examinations (AX350)

Tijdens de AXIOM macOS Examinations (AX350) training leren cursisten hoe ze apparaten kunnen onderzoeken die op het macOS besturingssysteem draaien.

Voor wie is deze training bedoeld?

Deze vierdaagse training is bedoeld voor digitaal rechercheurs en onderzoekers die bekend zijn met de principes van digitaal forensisch onderzoek en die hun kennis willen uitbreiden op het gebied van macOS en de forensische analyse van apparaten op basis van het APFS-bestandssysteem en AXIOM. We raden aan dat cursisten eerst de AXIOM Examinations (AX200) training afronden alvorens met deze training wordt gestart.

Wat leert u tijdens de training?

- De basisprincipes van het macOS besturingssysteem en het APFS-bestandssysteem inclusief de veranderingen in de beveiliging van macOS apparaten en wat de belangrijkste onderdelen van het macOS besturingssysteem zijn.
- Welke versleutelingsuitdagingen er zijn en hoe deze met behulp van Passware kunnen worden onderzocht.
- Welke verschillende macOS logbestanden er zijn en welke log artefacten kunnen worden aangetroffen.
- Wat de KnowledgeC database en de powerlog database inhouden die zijn opgeslagen op macOS.
- Welke internetartefacten er zijn.
- Welke specifieke gegevens van een gebruikersaccount van belang kunnen zijn voor een forensisch onderzoek.
- Hoe artefacten en bijlagen uit de standaard mailapplicatie Mail.App kunnen worden hersteld.
- Welke bruikbare informatie er aangetroffen kan worden op een desktop. Denk hierbij aan welke items zijn opgeslagen in de mac Dock, de toepassing van de menubalk, recente gebruikte items en thumbnails.
- Wat de Time Machine- en Snapshot functionaliteiten van macOS en het APFS-bestandssysteem inhouden.
- Hoe macOS clouddiensten gebruikt worden en welke databases de gegevensstromen tussen de cloud diensten en de hostcomputer regelen.

Extra informatie

Deze training is modulair opgebouwd. Bij elke module wordt er gebruik gemaakt van scenario's en hands-on oefeningen om de leerdoelen te versterken. Verder wordt de training in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Oxygen Forensic Bootcamp (OFBC)

De focus van deze driedaagse training ligt op het analyseren van de data en het maken van een rapport met Oxygen Forensic Detective. Het uitlezen van een mobile device (extractie) wordt in deze training slechts op

hoofdlijnen behandeld. Deelnemers leren tijdens de training met name hoe zij extracties van Android, Apple en andere datatypes importeren en analyseren.

Voor wie is deze training bedoeld?

Deze praktijkgerichte driedaagse training is bedoeld voor deelnemers die reeds basiskennis hebben van het acquireren en analyseren van mobiele apparaten zoals smartphones en iPads.

Wat leert u tijdens de training?

Deze training is een mix van theoretische en praktische sessies en wordt afgesloten met een oefening waarbij een grote zaak wordt onderzocht. Ondergenoemde aspecten komen daarbij aan de orde:

- Installatie en configuratie van de Oxygen Forensic Detective software.
- Interpretatie van de gebruikersinterface.
- Extractie en import opties van de software.
- Hoe de data te interpreteren.
- Onderzoek van categorieën zoals oproepen, contacten en accounts.
- Analyse van de tijdlijn, social media en foto's.
- Begrip van de ' Key Evidence Manager'.
- Categorisatie van gezichten (Facial recognition).
- Overige Oxygen tooling zoals Oxygen Maps, Oxygen Cloud Extractor etc.
- Keyword Search.
- Zoeken naar WiFi verbindingen en locaties.
- Zoeken naar wachtwoorden en tokens.
- Hoe om te gaan met back-ups.
- Data export en rapport functionaliteit.

Aan het einde van deze training hebben de deelnemers dus inzicht in de mogelijkheden omtrent het forensische platform Oxygen Forensic Detective. De deelnemers hebben kennis opgebouwd omtrent het uitlezen van apparaten (IOS, Android en KaiOS), extracten van cloud services, jailbreaken en meer. Daarnaast krijgen ze inzicht in alle analyse mogelijkheden in het platform en hoe dit kan worden verwerkt in een rapport.

Extra informatie

De training kan zowel in het Engels als Nederlands gegeven worden en kan zowel klassikaal als online worden verzorgd.

Oxygen Forensic Advanced Analysis (OFAA)

Deze hands-on training is een vervolg op de Oxygen Forensic Bootcamp Training (OFBC) en gaat dieper in op de functionaliteiten van Oxygen Forensic Detective. Het doel van de training is om diepgaande kennis van mobiele forensics te verkrijgen aan de hand van deze tool.

Voor wie is deze training bedoeld?

Deze driedaagse training is geschikt voor digitaal rechercheurs en onderzoekers die zich verder willen specialiseren in het verzamelen en analyseren van mobiele data afkomstig van onder meer smartphones en iPads. Het is een vereiste dat men voorafgaand aan deze training eerst de Oxygen Forensic Bootcamp Training (OFBC) heeft gevolgd.

Wat leert u tijdens de training?

Na afloop van deze training zijn cursisten op de hoogte van de functionaliteiten die Oxygen Forensics te bieden heeft. Zo weten ze onder meer hoe ze met behulp van deze technologie data kunnen analyseren, parsen en herstellen. Ook hebben ze geleerd te werken met geavanceerde tools zoals Call Data Record expert, SQLite, Propertiy list viewer en Oxygen Maps. Verder leren de deelnemers IoT apparaten te onderzoeken en gegevens uit meerdere bronnen samen te voegen en te correleren voor hun onderzoek.

Extra informatie

De training wordt in het Engels gegeven en kan zowel klassikaal als online worden verzorgd.

Oxygen Forensic Cloud Extraction (OFCE)

De focus van deze training ligt op het verzamelen van data uit de cloud met behulp van Oxygen Forensic KeyScout. Tijdens de training komen een aantal verschillende platformen aan bod waaronder Apple en Google.

Voor wie is deze training bedoeld?

Deze eendaagse training is geschikt voor digitaal rechercheurs en onderzoekers die al bekend zijn met Oxygen Forensic Detective en die willen leren hoe ze een onderzoek in de cloud kunnen uitvoeren met KeyScout.

Wat leert u tijdens de training?

- Cloud-gebaseerde repositories te extraheren door gebruik te maken van Oxygen Forensic KeyScout en Oxygen Forensic Detective met als doel inloggegevens en tokens te verkrijgen om toegang tot cloud platformen te krijgen.
- Welke problemen zich bij tweefactor authenticatie kunnen voordoen.
- Hoe een WhatsApp database hersteld kan worden.
- Welke type gegevens verzameld kunnen worden op platformen zoals Amazon, Google, WhatsApp en Apple services met behulp van de Oxygen Forensic Cloud Extractor.
- Hoe met behulp van Oxygen Forensic KeyScout een dead box recovery kan worden uitgevoerd van harde schijven afkomstig van computers, forensische images en live machines.
- Hoe zoekpaden en zoekprofielen op maat gemaakt kunnen worden en hoe deze resultaten vervolgens opgeslagen kunnen worden voor verdere analyse met Oxygen Forensic Detective.

Extra informatie

De training kan zowel in het Engels als Nederlands worden gegeven en kan zowel klassikaal als online worden verzorgd.

DataExpert

Oxygen Forensic Extraction in a Box (XiB)

Deze driedaagse hands-on training is gericht op het extraheren van data van mobiele telefoons. De focus ligt op de data extractie van Android, Apple en KaiOS toestellen, maar ook Drones, SD-cards en SIM-Cards worden onderzocht.

Iedere cursist krijgt bij aanvang van de cursus de beschikking over een plastic doosje met 10 verschillende telefoons als basis, vandaar de titel van de training. Er wordt gebruik gemaakt van de Oxygen Forensic Extractor, een onderdeel van Oxygen Forensic Detective.

Voor wie is deze training bedoeld?

Deze training is geschikt voor cursisten met een basiskennis van mobile forensics.

Wat leert u tijdens de training?

- Logische, fysieke en OxyAgent extractiemethoden
- Basics van Full Disk encryption en File-based encryption
- Decryptie-, bypass, Emergency Download (EDL) en ADB-technieken

Extra informatie

Deze training wordt in het Engels gegeven.

Teel Technologies Advanced Flasher Box & Bootloader Forensics

Tijdens deze vijfdaagse praktijkgerichte training leren rechercheurs met behulp van de meest gangbare Flasher Box en Bootloader tools het geheugen van mobiele apparaten te decrypten en uit te lezen. Deze techniek is vooral zinvol daar waar standaard tooling niet toereikend is. Deze methode is zowel toepasbaar op high-end Android apparaten zoals bijvoorbeeld Samsung Smartphones, als op simpele mobiele telefoons met MediaTek of Chinese chipsets.

Flasher Box

Tijdens dit gedeelte van de training krijgen de studenten een overzicht van de meest courante Flasher Box tools. Daarnaast gaan de studenten zelf aan de slag met het installeren en gebruiken van deze tools. Daarbij maken ze gebruik van diverse modellen die na afloop van de training mogen worden behouden.

Bootloader

Tijdens dit gedeelte van de training leren de studenten hoe partities op mobiele apparaten kunnen worden benaderd voor unlock of bypass doeleinden. Er wordt geleerd hoe ADB Commands toe te passen, het identificeren van FRP-locks op een mobiele telefoon en hoe deze te omzeilen, het gebruik van CWM en TWRP om een mobiel apparaat te unlocken en het geheugen te benaderen of te kopiëren.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor rechercheurs die ervaring hebben op het gebied van Mobile Forensics en hun kennis op het gebied van analyse van mobiele apparaten willen vergroten.

Wat leert u tijdens de training?

Aan het eind van deze training zijn cursisten in staat zelfstandig mobiele apparaten te benaderen en te decrypten met behulp van geavanceerde technieken. Iedere student ontvangt na afloop een complete Flasher en Unlock kit bestaande uit een NCK dongle, een XTC clip met Y-kabel en een EFT dongle.

Extra informatie

De training wordt in het Engels gegeven en wordt klassikaal verzorgd.

Teel Technologies Board Level Repair for the Digital Forensic Examiner

Er is een grote verscheidenheid aan tooling beschikbaar voor het uitlezen en analyseren van mobiele apparaten. Hoewel er veel mogelijk is, zijn er ook beperkingen. Defecte smartphones kunnen vaak alleen nog op boardlevel niveau worden uitgelezen. Data extractie vindt dan plaats direct op de chip. Dit betekent wel dat het betreffende apparaat dient te worden gedemonteerd. Tijdens deze praktijkgerichte training leren cursisten diagnosevaardigheden, probleemoplossingen en de nieuwste reparatietechnieken met de modernste apparatuur.

Voor wie is deze training bedoeld?

Deze vijfdaagse training is geschikt digitaal rechercheurs, digitaal specialisten en onderzoekers die te maken krijgen met beschadigde gegevensdragers tijdens hun forensische onderzoek.

Wat leert u tijdens de training?

- Gegevens aanwezig op een beschadigde gegevensdrager (denk bijv. aan waterschade) te herstellen.
- Welke hulpmiddelen ingezet kunnen worden om defecte apparaten te herstellen.
- Te herkennen wanneer gegevens onherstelbaar zijn.
- De werking van printplaten.
- De werking van Surface Mount Components (SMCs).
- Precieze soldeertechnieken, reparatie en z.g. reballing.
- Schema's te lezen.
- En nog veel meer!

Extra informatie

De training wordt in het Engels gegeven en wordt klassikaal verzorgd.

DataExpert

Teel Technologies Chip-Off 2.0 Forensics

Tijdens de vijfdaagse Teel Tech Chip-Off Forensics training leren cursisten hoe ze geheugenchips uit mobiele apparaten zoals smartphones kunnen verwijderen, prepareren en uitlezen om vervolgens met behulp van specialistische apparatuur de data te verkrijgen.

In de eerste helft van de training ligt de focus op het begrijpen van de opbouw van de apparaten en hoe het beste de chip verwijderd kan worden zonder de chip te beschadigen. Daarnaast verkrijgen de cursisten inzicht in de verschillende geheugenstructuren van mobiele apparaten (mobiele telefoons, tablets, SSD-harde schijf enz.) en hoe de Chip-Off kan worden gebruikt om gegevens te verzamelen.

In de tweede helft van de training leren cursisten de basisprincipes van de geheugenstructuur en hoe ze beschikbare hulpmiddelen kunnen gebruiken om het geheugen van de chip te lezen. Cursisten kunnen de verkregen kennis in de praktijk brengen door te oefenen op een BlackBerry toestel die geladen is met gegevens.

Voor wie is deze training bedoeld?

Deze Chip-Off training is bedoeld voor cursisten die bekend zijn met het concept van ruwe data, ruime ervaring hebben in het analyseren hiervan en hun kennis van Chip-Off methodieken willen vergroten.

Wat leert u tijdens de training?

Na het volgen van deze training beschikken de cursisten over de volgende competenties:

- Het verwijderen op juiste wijze van een BGA-chip van een apparaat.
- Behandeling en voorbereiding van de chip voor uitlezing.
- Het uitlezen van de chip om gegevens te verkrijgen.
- Het toepassen van hulpmiddelen en technieken om de aangetroffen informatie te decoderen.
- Praktische kennis over het Chip-Off proces van een geblokkeerde niet-versleutelde BlackBerry en vervolgens het gebruik van forensische software om de data dump te maken en analyseren.

Extra informatie

De training wordt in het Engels gegeven en wordt klassikaal verzorgd.

Teel Technologies Embedded Hardware Acquisition & Analysis

Tijdens deze hands-on training ligt de focus op processen die gebruikt kunnen worden om toegang te krijgen tot digitale data op fysiek niveau van gegevensdragers. Deze bronnen zijn onder meer:

- IOT apparaten
- Smart TV's
- Voertuigsystemen
- Drones
- Skimmers/Shimmers

Voor wie is deze training bedoeld?

Deze vijfdaagse training is bedoeld voor digitaal rechercheurs, digitaal specialisten en onderzoekers die te maken krijgen met digitale data op fysieke gegevensdragers tijdens een onderzoek.

Wat leert u tijdens de training?

- Basiskennis over hoe elektronica werkt in relatie tot technieken die in deze training worden gebruikt.
- Welke (open source) bronnen en commerciële tools ingezet kunnen worden.
- Hoe technieken als JTAG, ISP en Chip-Off aan te passen om data te verzamelen vanuit bronnen zoals embedded code en het flash memory van controller chips.
- Hoe de verkregen data te analyseren op zoek naar bewijsmateriaal en sporen van malware.

Extra informatie

De training wordt in het Engels gegeven en wordt klassikaal verzorgd.

Teel Technologies JTAG Forensic

Tijdens deze vijfdaagse training leren rechercheurs hoe de informatie van vergrendelde mobiele telefoons te ontsluiten gebruikmakend van het JTAG proces. Hierbij wordt een toestel geheel uit elkaar gehaald en op fysiek niveau benaderd. Nadat de data is gekopieerd, leert de cursist hoe het wachtwoord te achterhalen om vervolgens de gevonden informatie te decoderen. Tenslotte wordt het toestel weer teruggebracht in de originele staat en kan het met behulp van het gevonden wachtwoord worden ontgrendeld. Het JTAG proces kan worden toegepast in de volgende situaties:

- Vergrendelde Android toestellen met USB debugging uitgeschakeld.
- Vergrendelde Windows toestellen.
- Vergrendelde toestellen met niet gangbare besturingssystemen.
- Toegang tot het fysieke geheugen van een toestel indien dit niet door tooling wordt ondersteund.
- Beschadigde of vernielde toestellen.

Voor wie is deze training bedoeld?

Deze JTAG training voor gevorderden is bedoeld voor digitaal rechercheurs met goede kennis van Computer

DataExpert

Forensics en ruime ervaring met onderzoek van mobiele apparaten die hun technische kennis willen verdiepen.

Wat leert u tijdens de training?

Aan het eind van deze training zijn cursisten in staat om een werkende mobiele telefoon volledig te ontmantelen, de relevante informatie uit te lezen en vervolgens het toestel weer in elkaar te zetten op non-destructieve wijze. Daarnaast leren de cursisten hoe de verschillende Mac kopiebestanden en kopieën gemaakt met andere tools of besturingssystemen geïdentificeerd kunnen worden. Ook de locatie in het bestandssysteem, hoe informatie te verzamelen op forensisch correcte wijze en het breken van wachtwoorden komen aan de orde.

Extra informatie

De training wordt in het Engels gegeven en wordt klassikaal verzorgd.

Teel Technologies ISP Forensic

Tijdens deze vijfdaagse training leren rechercheurs met behulp van z.g. In-System Programming (ISP) extracties uit te voeren. Deze methode maakt het mogelijk om rechtstreeks toegang te krijgen tot het eMMC-geheugen van een mobiel apparaat. eMMC is het meest voorkomende type geheugen dat wordt toegepast in chips van de huidige smartphones. Gedurende het ISP proces hoeft de chip niet te worden verwijderd, waardoor het originele bewijs intact blijft. Aan het begin van de training krijgen de cursisten een aantal telefoons uitgereikt om chip-off extracties op te oefenen, te leren over backtracing en connectiepunten en data-extracties uit te voeren.

Voor wie is deze training bedoeld?

Deze ISP training is bedoeld voor rechercheurs die ervaring hebben in Chip-Off en soldeertechnieken en hun kennis op het gebied van analyse van mobiele apparaten willen vergroten.

Wat leert u tijdens de training?

Aan het eind van deze training zijn cursisten in staat zelfstandig ISP extracties uit te voeren en de resultaten van de verschillende extracties met elkaar te vergelijken. Hoewel er een basisvaardigheid in het solderen van PCB's wordt gevraagd bij aanvang van de training, zal er veel worden geoefend in het solderen van weerstanden en condensators op en van de printplaat.

Extra informatie

De training wordt in het Engels gegeven en wordt klassikaal verzorgd.

Teel Technologies SQLite Forensics

Zowel Google's Android OS als Apple's iOS zijn dominante spelers in de huidige markt van mobiele telefoons. Hoewel deze twee bedrijven rivalen zijn, met sterk verschillende file systems, hebben ze één ding gemeen; beide gebruiken SQLite als opslag voor gebruikersgegevens. SQLite is een bibliotheek die een onafhankelijke,

serverloze, zero-configuratie SQL database engine implementeert. Tijdens deze training leren cursisten hoe ze op een basis dataniveau SQLite databases kunnen analyseren en herstellen. Na afloop van deze training zijn onderzoekers met deze kennis in staat om meer dan 99% van de data die ze tegenkomen op mobiele apparaten te analyseren.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor digitaal rechercheurs, digitaal specialisten en onderzoekers die te maken krijgen met mobiele apparaten tijdens hun forensische onderzoek.

Wat leert u tijdens de training?

- Hoe SQLite werkt op byte-niveau.
- Wat de vijf meest voorkomende locaties zijn om SQLite gegevens te herstellen.
- Hoe rapportgegevens te valideren.
- Wat de verschillende soorten SQLite datacomponent types zijn.
- Het reverse engineeren van een SQLite database.
- Het eenvoudig converteren en identificeren van vrijwel elk data format.
- SQLite BLOB gegevens weer te geven in een forensisch programma.
- Het herstellen van gegevens van .WAL en .journal bestanden.
- Het snel genereren van rapporten van een SQLite database met extern gekoppelde afbeeldingen.
- SQLite Record herstel.
- Het handmatig parsen van Write-Ahead Logs en Journal bestanden.
- SQLite Payload onderzoek/SQLite Data Construct parsing.
- Handmatig SQLite gegevens herstellen.
- SQLite encryptie.
- Het gebruik van simulaties om gegevens te testen, verifiëren en decoderen.

Extra informatie

De training wordt in het Engels gegeven en wordt klassikaal verzorgd.

Open Source Intelligence

Het internet bevat een onnoemelijke hoeveelheid aan data. Deze data kan van toegevoegde waarde zijn in onderzoeken. Door gebruik te maken van Open Source Intelligence (OSINT) kan de onderzoeker/rechercheur/analist data vergaren die voor het onderzoek van belang is. Zo kunnen bijvoorbeeld sociale netwerken in beeld gebracht worden, nieuwsberichten worden verzameld en geanalyseerd en kan er inzicht verkregen worden in publicaties op fora.

Tijdens de OSINT trainingen leren onderzoekers/ rechercheurs/analisten de juiste vaardigheden om data van het publieke internet te verzamelen en deze te duiden. Welke informatie is juist, welke gegevens zijn betrouwbaar en hoe kunnen de gevonden resultaten goed worden vastgelegd? Deze vragen worden tijdens de trainingen beantwoord.

OSINT

Leerlijn OSINT Compleet

OSINT is in de afgelopen jaren een belangrijk middel voor informatie- en datavergaring geworden. Echter beslaat het meer dan alleen het internet en gaat het verder dan een simpele zoekopdracht in een zoekmachine. In deze leerlijn krijgen de cursisten een breed palet van competenties aangereikt. De cursisten leren onafhankelijk van tooling en door middel van eigen skills een volledig OSINT onderzoek van “a tot z” te plannen, het onderzoek uit te voeren, de opgedane informatie in de juiste context te interpreteren en vervolgens te rapporteren.
De leerlijn OSINT Compleet bestaat uit drie losse trainingen waarbij het kennisniveau iedere training verder wordt verhoogd en de competenties worden uitgebouwd. Zo worden alle aspecten van OSINT behandeld, zowel in methodiek als techniek.
Deze leerlijn bestaat uit de trainingen:

- OSINT Basis – 3 dagen
- OSINT Advanced – 3 dagen
- OSINT Technical – 3 dagen

De trainingen zijn opeenvolgend, maar worden los van elkaar gepland. Hierdoor krijgen de deelnemers de gelegenheid tussentijds de lesstof te laten bezinken en te reflecteren. Dit kan door middel van de informatie op het e-learning platform en door het toepassen van de kennis in het werkveld. Daarnaast is het mogelijk één of twee trainingen los van de leerlijn te volgen wanneer dit toereikend is voor de functie die de cursist bekleedt.
Elke training is afzonderlijk van elkaar geaccrediteerd bij het SPEN/CPION. Dit houdt in dat de cursist na het succesvol afronden van elke training een erkende titel en diploma ontvangt.

Voor wie is deze training bedoeld?

Deze leerlijn is geschikt voor eenieder die het internet gebruikt bij (opsporings)onderzoeken, waaronder politie en overige opsporings- en veiligheidsdiensten, themaonderzoekers, analisten bij banken (CDD, KYC, AML) en particulier onderzoekers.

Wat leert u tijdens de training?

Na het volgen van de OSINT trainingen Basis, Advanced en Technical is de cursist in staat om eenvoudige en complexe(re) OSINT onderzoeken te plannen, uit te voeren en te rapporteren. Hierbij heeft hij/zij oog voor mogelijke afbreukrisico’s en zijn/haar eigen veiligheid. Ook weet de cursist eigen tooling te bouwen om zo op basis van eigen skills onderzoek uit te voeren. Voor de verdere inhoud van de trainingen verwijzen wij u naar de individuele trainingen.

Extra informatie

De trainingen in deze leerlijn worden ondersteund door het e-learning platform van DataExpert. Hier kunnen deelnemers kennisnemen van de theorie door middel van tekst en korte video’s. Verder kan de training zowel online als klassikaal worden verzorgd.

DataExpert

OSINT Basis - Registered OSINT Practitioner ®

Door gebruik te maken van Open Source Intelligence, ook wel internet rechercheren genoemd, is het mogelijk om tijdens fraude-, cybercrime- en/of opsporingsonderzoeken relevante gegevens te vinden uit digitale open bronnen.

Tijdens de training “OSINT Basis” leren de deelnemers de basisvaardigheden die benodigd zijn om een goed onderzoek op het internet uit te voeren. Na het volgen van deze training kunnen de deelnemers een onderzoek uitvoeren op het internet, de informatie die daarbij wordt aangetroffen duiden en deze vervolgens in de juiste context interpreteren en verbaliseren/rapporteren.

Deze training is een geaccrediteerde SPEN-registeropleiding. Indien u een eindtoets aflegt en deze succesvol afrondt, ontvangt u een diploma van de Stichting Permanente Educatie Nederland (SPEN) en mag u de titel ‘Registered OSINT Practitioner ®’ (afgekort ROP) voeren. Dit houdt tevens in dat u wordt ingeschreven in het Abituriëntenregister van het Centrum voor Post Initieel Onderwijs Nederland (CPION) en Persoonlijke Educatie (PE) punten ontvangt.

Voor wie is deze training bedoeld?

Deze driedaagse training is geschikt voor eenieder die het internet gebruikt bij (opsporings)onderzoeken, waaronder politie en overige opsporings- en veiligheidsdiensten, themaonderzoekers, analisten bij banken (CDD, KYC, AML), particulier onderzoekers en meer.

Wat leert u tijdens de training?

Aan het einde van deze training heeft de deelnemer inzicht in de mogelijkheden van het internet en digitalisering in de opsporingswereld. De deelnemer heeft geleerd effectief gebruik te maken van zoekmachines, het onderzoeken van afbeeldingen, e-mailheaders en de eerste stappen gezet in onderzoek op social media (SOCMINT). Ook weet de deelnemer binnen websites te zoeken, waar men gegevens kan vorderen (indien bevoegd) en welke technieken er zijn om anoniem te opereren.

Extra informatie

Deze training is onderdeel van de leerlijn OSINT Compleet waartoe ook de trainingen OSINT Advanced en Technical behoren. De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online. Verder is de training modulair opgebouwd, waardoor het ook mogelijk is om een maatwerk training samen te stellen met bijpassende casuïstiek.

OSINT Advanced - Registered OSINT Specialist ®

Tijdens de vervolgtraining “OSINT Advanced” leren de deelnemers extra vaardigheden die benodigd zijn om een diepgaand onderzoek op het internet uit te voeren. Na het volgen van deze training kunnen de deelnemers een uitgebreid onderzoek uitvoeren op zowel het internet als het dark web. Zij kunnen de informatie die ze daarbij aantreffen duiden en deze vervolgens in de juiste context interpreteren en verbaliseren/rapporteren.

Deze training is een geaccrediteerde SPEN-registeropleiding. Indien u een eindtoets aflegt en succesvol afrondt, ontvangt u een diploma van de Stichting Permanente Educatie Nederland (SPEN) en mag u de titel ‘Registered OSINT Specialist ®’ (afgekort ROS) voeren. Dit houdt tevens in dat u wordt ingeschreven in het Abituriëntenregister van het Centrum voor Post Initieel Onderwijs Nederland (CPION) en Persoonlijke Educatie (PE) punten ontvangt.

Voor wie is deze training bedoeld?

Deze driedaagse training is geschikt voor eenieder die het internet gebruikt bij (opsporings)onderzoeken, waaronder politie en overige opsporings- en veiligheidsdiensten, themaonderzoekers, analisten bij banken (CDD, KYC, AML), particulier onderzoekers en meer. Wel adviseren wij de deelnemer om eerst de training OSINT Basis succesvol te hebben afgerond.

Wat leert u tijdens de training?

Aan het einde van deze training heeft de deelnemer inzicht in de mogelijkheden van diepgaander onderzoek op het internet en het darknet. De deelnemer heeft geleerd effectief gebruik te maken van geavanceerde zoektechnieken, geolocatie onderzoek en heeft vergevorderde stappen gezet in onderzoek op social media (SOCMINT). Ook weet de deelnemer virtuele onderzoeksomgevingen op te zetten en een eerste aanzet te maken tot onderzoek naar cryptovaluta, waaronder Bitcoin.

Extra informatie

Deze training is onderdeel van de leerlijn OSINT Compleet waartoe ook de trainingen OSINT Basis en Technical behoren. De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online. Verder is de training modulair opgebouwd, waardoor het ook mogelijk is om een maatwerk training samen te stellen met bijpassende casuïstiek.

OSINT Technical - Registered OSINT Technical Specialist ®

Tijdens de vervolgtraining “OSINT Technical” leren de deelnemers de ‘technische’ vaardigheden die benodigd zijn om een diepgaand onderzoek op het internet uit te voeren door gebruik te maken van Linux, scrapen en andere hulpmiddelen. Na het volgen van deze training kunnen de deelnemers een deels geautomatiseerd onderzoek uitvoeren op het internet met behulp van tools, virtual machines en Python.
Deze training is een geaccrediteerde SPEN-registeropleiding. Indien u een eindtoets aflegt en succesvol afrondt, ontvangt u een diploma van de Stichting Permanente Educatie Nederland (SPEN) en mag u de titel

DataExpert

‘Registered OSINT Technical Specialist ®’ (afgekort ROTS) voeren. Dit houdt tevens in dat u wordt ingeschreven in het Abituriëntenregister van het Centrum voor Post Initieel Onderwijs Nederland (CPION) en Persoonlijke Educatie (PE) punten ontvangt.

Voor wie is deze training bedoeld?

Deze driedaagse training is geschikt voor eenieder die het internet gebruikt bij (opsporings)onderzoeken, waaronder politie en overige opsporings- en veiligheidsdiensten, themaonderzoekers, analisten bij banken (CDD, KYC, AML), particulier onderzoekers en meer. Wij adviseren de deelnemers om eerst de training OSINT Basis en OSINT Advanced succesvol af te ronden voordat men deelneemt aan deze training.

Wat leert u tijdens de training?

Aan het einde van deze training heeft de deelnemer inzicht in de mogelijkheden van diepgaander (technisch) onderzoek op het internet. De deelnemer heeft inzicht in poorten en protocollen en weet effectief gebruik te maken van de Linux Command Line. Ook kan de deelnemer Python scripts en scrapers inzetten om geautomatiseerd onderzoeken uit te voeren met behulp van onder andere API’s.

Extra informatie

Deze training is onderdeel van de leerlijn OSINT Compleet waartoe ook de trainingen OSINT Basis en Advanced behoren. De training kan in het Nederlands of Engels worden verzorgd. Verder is de training modulair opgebouwd, waardoor het ook mogelijk is om een maatwerk training samen te stellen met bijpassende casuïstiek.

OSINT Onl1ne G4ming

De online gaming community groeit harder dan ooit. Alleen al in Europa zijn er meer dan 715 miljoen gamers (bron: Ipsos). Hierdoor zijn er de laatste jaren steeds meer platformen ontstaan of geëvolueerd om deze online communities te ondersteunen. Deze platformen worden echter ook meer en meer ingezet door (cyber)criminelen om criminele activiteiten te ondersteunen, zoals uitbuiting, witwassen, fraude of hacking. Ongemerkt gaan er miljoenen euro's rond in deze relatief onzichtbare wereld.

Voor veel onderzoekers is dit een nieuwe (virtuele) wereld waarin opsporingskansen zich voordoen, mits men weet hoe deze te benutten. Tijdens de training worden onderwerpen als terminologie, online communities als Reddit, underground (gaming) markets en platformen als Twitch behandeld.

Dus of u nu een n00b bent op het gebied van online gaming of een pro met serieuze skills, deze training onder leiding van een van onze dungeon masters, laat u op veilige wijze uw XP farmen om de OSINT- skills naar het volgende level te krijgen.

Voor wie is deze training bedoeld?

Deze tweedaagse training is geschikt voor eenieder die het internet gebruikt bij (opsporings)onderzoeken, waaronder politie, defensie en overige opsporings- en veiligheidsdiensten, themaonderzoekers, analisten bij banken (CDD, KYC, AML), verzekeraars, particulier onderzoekers en meer.

Wij adviseren de deelnemers om eerst de training OSINT Basis en OSINT Advanced succesvol af te ronden voordat men deelneemt aan deze training.

Wat leert u tijdens de training?

Aan het einde van de training OSINT Online Gaming heeft de deelnemers inzicht verkregen in de meest populaire online gaming platformen en de daaraan gelieerde communities en social media platformen. De deelnemer herkent de opsporingskansen en uitdagingen die een dergelijk onderzoek met zich meebrengt en weet deze te benutten indien mogelijk. Daarnaast is de deelnemer in staat om een onderzoek uit te voeren op diverse online gaming platformen en de bevindingen te rapporteren.

Maltego Fundamentals

Maltego is wereldwijd een van de meest gebruikte OSINT-tools voor het verzamelen, verbinden en analyseren van online openbare informatie. De software kenmerkt zich door de grafische link analyse interface en de vele transforms die het mogelijk maken om andere tooling door middel van API toegang te integreren, waaronder Virus Total, PiPl, ShadowDragon, Att&ck en meer. Aanvullend kan geëxporteerde data uit i2 Analyst's Notebook verrijkt worden met behulp van Maltego en kan verdere analyse vervolgens plaatsvinden in i2 Analyst's Notebook op basis van verkregen data uit Maltego.

DataExpert

Tijdens de eendaagse Maltego Fundamentals training worden deelnemers voorzien van de nodige tips, tricks en hands-on ervaring, zodat men de software effectief leert gebruiken gedurende onderzoeken op het gebied van o.a. OSINT, due diligence of Cyber Threat Intelligence (CTI).

De training wordt gegeven op interactieve wijze, waarbij theorie en praktijk met elkaar worden afgewisseld. Onderwerpen worden toegelicht, waarna de deelnemers dit zelfstandig of in duo's oefenen door middel van opdrachten of cases.

Voor wie is deze training bedoeld?

Deze training is bedoeld voor gebruikers die geen tot weinig ervaring hebben met het gebruik van Maltego software of de kennis hierover willen opfrissen.

Wat leert u tijdens de training?

- De werking en installatie van Maltego.
- OpSec (Operational Security) & Maltego.
- Het werken met de user interface van Maltego.
- Het effectief vergaren van data met Maltego (entities & collections).
- De werking van (en werken met) machines en transforms.
- Het verkrijgen van inzicht tussen standaard hubs/transforms t.o.v. commerciële hubs/transforms en de impact op het onderzoek.
- Importeren en exporteren van data met Maltego.
- Hoe een gericht onderzoek met Maltego kan worden uitgevoerd.

Extra informatie

De training wordt klassikaal gegeven en kan in het Nederlands of Engels worden verzorgd. Ook is het mogelijk om maatwerk toe te passen, neem voor meer informatie hierover contact met ons op.

Python

Tijdens deze training leren deelnemers programmeren in de programmeertaal Python. Deze dynamische programmeertaal is 'easy to learn en hard to master'. Door zijn simpele opzet is Python de go-to programmeertaal voor beginners.

Met Python is het mogelijk relatief simpele taken en analyses uit te voeren, webservers te draaien, artificial intelligence toe te passen en nog veel meer! Leer tijdens deze vierdaagse training als beginnende Python programmeur de fijne kneepjes van deze programmeertaal.

Voor wie is de training bedoeld?

De training is bedoeld voor deelnemers die al enige technische kennis van computers hebben en hun skill-set willen upgraden met een programmeertaal.

Wat leert u tijdens de training?

- De Python Interpreter.
- De basis van de Python taal.
- De basisbeginselen van het lezen en schrijven van bestanden.
- Het werken met ‘packages’.
- Verschillende programmeeromgevingen beheren.
- Analyseren van een uitgebreide logfile.
- Het maken van een web crawler.

Extra informatie

De training kan in het Nederlands of Engels worden verzorgd; zowel klassikaal als online.

Refresher training

De tijdens een cursus opgedane kennis en vaardigheden zakken vaak weer weg na verloop van tijd. Daarnaast zijn er altijd veel nieuwe ontwikkelingen binnen het vakgebied “OSINT” die van toegevoegde waarde zijn om te delen. Een Refresher training is een uitstekende mogelijkheid om deze kennis en vaardigheden in korte tijd weer op te halen.

Fris de belangrijke punten uit onze OSINT training(en) op en zet deze kennis en software in voor het oplossen van vraagstukken.

DataExpert

Private Training

Naast onze standaard trainingen bieden we ook trainingen op maat aan. Hierbij kijken we samen met u naar de wensen en behoeften van uw organisatie en passen indien nodig het cursusmateriaal aan. Bij specifieke wensen denken we graag met u mee.

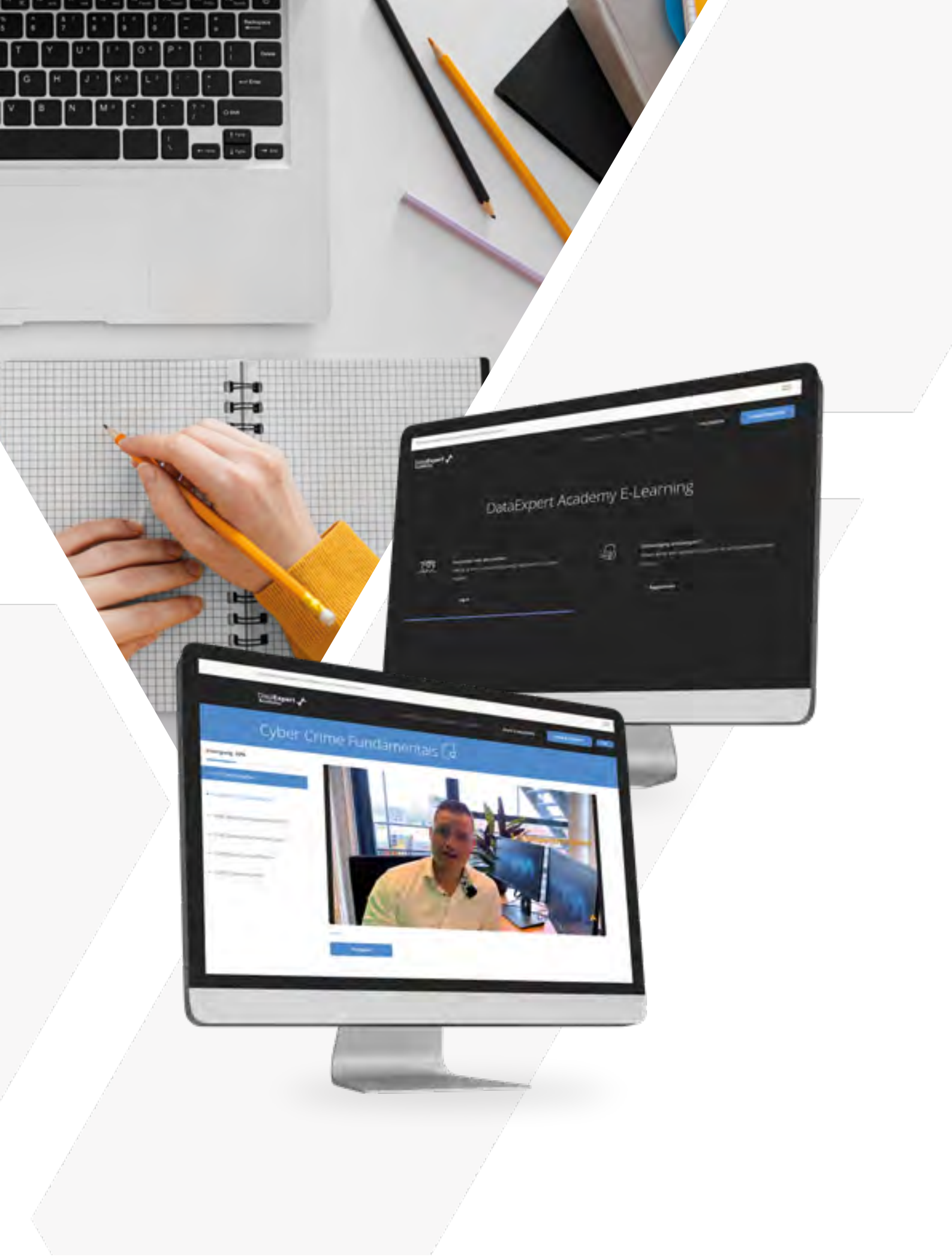
Bij een training op maat, kunt u denken aan:

- Training voor één of meer deelnemers van dezelfde organisatie.
- Training wordt volledig afgestemd op de wensen van de cursisten of organisatie.
- Training kan plaatsvinden bij u op locatie of bij DataExpert in Veenendaal.
- Inhoud van de training kan vooraf en in overleg met de trainer afgestemd worden.
- Bij de training kunnen eigen data (mits de AVG regelgeving dat toestaat) of voorbeelddata gebruikt worden.
- De duur van de training wordt samen met de trainer vooraf vastgelegd en is mede afhankelijk van de hoeveelheid stof en het aantal cursisten.

Neem voor meer informatie over de verschillende mogelijkheden contact met ons op!

> THE GREAT AIM OF EDUCATION IS NOT KNOWLEDGE BUT ACTION.
>
> HERBERT SPENCER

> DEVELOP A PASSION FOR LEARNING. IF YOU DO, YOU WILL NEVER CEASE TO GROW.
>
> ANTHONY J. D'ANGELO


DataExpert Academy E-Learning
Cyber Crime Fundamentals

Het DataExpert e-learning platform

Bij DataExpert hechten wij veel waarde aan duidelijke en heldere kennisoverdracht. Dit doen wij door een combinatie van leervormen aan te bieden.

Pre-learning

Een aantal trainingen uit ons portfolio zijn aangevuld met één of meer pre-learning modules. Dit zijn self-paced, online lessen die te volgen zijn in het e-learning platform. Met deze modules kan de cursist in eigen tijd kennis opdoen alvorens deel te nemen aan een klassikale training.

Self paced training

Via ons e-learning platform bieden wij tevens e-learning only trainingen aan. Dit zijn trainingen welke de cursist in eigen tijd en op eigen tempo kan volgen. In deze training vindt de cursist een reeks instructies en opdrachten in ons platform.

Video materiaal

Veel van onze trainingen zijn naast schriftelijk materiaal ook voorzien van video's. Deze video's maken de blended learning ervaring compleet. Voor een select aantal trainingen, bijvoorbeeld in het cybercrime domein, zijn alle modules voorzien van tekst én videomateriaal.

Knowledge base

Wij bieden verschillende trainingen klassikaal aan. Deze verlopen via een gepland programma en worden geleid door een professionele trainer. Ons e-learning platform vervult in deze opzet de rol van knowledge base; al het trainingsmateriaal is hier terug te lezen.

Toetsing

Indien van toepassing sluit de student in het e-learning platform les modules af middels een toets. Deze toetsen zijn multiple choice of open opdrachten. Van een multiple choice toets wordt de uitslag direct bekend en geregistreerd bij de voortgang. In het geval van een opdracht zijn de instructies ervoor in het platform te vinden.

DataExpert

Digital badges

Een training vergt naast tijd, de nodige inspanning en aandacht. Daarbij heeft u nieuwe vaardigheden en methodieken verworven die u direct kunt toepassen in uw onderzoek. Naast het ontvangen van een diploma of certificaat, vinden we bij DataExpert dat dit extra beloond en getoond mag worden. DataExpert biedt daarom cursisten voor een groot deel van onze trainingen een Digitale Badge aan. Elke opleiding of training heeft zijn eigen leerdoelen en daarom ook zijn eigen badge.

Cybercrime

Analytics

Digital Forensics

Open Source Intelligence

Notities

Voor meer informatie:

DataExpert B.V.
Vendelier 65
3905 PD Veenendaal

+31 (0)318 543173
training@dataexpert.nl

www.dataexpert.nl