

Keuzedeel mbo

Oriëntatie op digitaal forensisch onderzoek

gekoppeld aan één of
meerdere kwalificaties mbo

Code

K0360

Penvoerder: Sectorkamer ICT en creatieve industrie
Gevalideerd door: Sectorkamer ICT en creatieve industrie
Op: 10-11-2015

1. Algemene informatie

D1: Oriëntatie op digitaal forensisch onderzoek

Studielast

720

Beroepsvereisten

Nee

Certificaten

Ja

Scholingsbehoefte/landelijke herkenbaarheid

Het keuzedeel Oriëntatie op digitaal forensisch onderzoek gaat in op het inventariseren van digitale sporen en het veiligstellen van onderzoeksmateriaal. Ook het verwerken en uitvoeren van onderzoek op onderzoeksmateriaal komt aan bod. Hiermee specialiseert de beroepsbeoefenaar zich in het beroep digitaal forensisch onderzoeker. Deze specialisatie biedt de ICT-beheerder en Netwerk- en mediabeheerder meer kansen op de arbeidsmarkt. Daarnaast biedt het een oriëntatie op de doorstroommogelijkheid naar een functie op hbo-niveau (Network Forensics Research).

Ingangsdatum certificaat

01-10-2016

Gekoppeld aan kwalificatie(s)

Zie bijlage op www.s-bb.nl/kwalificatiedossiers

Toelichting

Met dit keuzedeel verdiept de leerling zich in het vakgebied Digitaal forensisch onderzoek.

De kern van het keuzedeel is het inventariseren van digitale sporen, het veiligstellen van digitaal onderzoeksmateriaal en het verwerken en uitvoeren van onderzoek op onderzoeksmateriaal. Het preventief handelen staat centraal. De beginnend beroepsbeoefenaar moet zich voortdurend de vraag stellen of het materiaal juist en volledig is, of het voldoet aan het subsidiariteits- en proportionaliteitsbeginsel en of het juridisch gerechtvaardigd is om het materiaal te onderzoeken. De beginnend beroepsbeoefenaar staat regelmatig voor de vraag welk hulpmiddel geëigend is. Inzet van verkeerde hulpmiddelen, of verkeerd gebruik van hulpmiddelen, kan tot een onjuiste conclusie leiden. Wat als gevolg kan hebben dat er te zware middelen worden ingezet.

Relevantie van het keuzedeel

Dit keuzedeel is een verdieping op kwalificatiedossier ICT-beheer. Hiermee specialiseert de beginnend beroepsbeoefenaar zich in het beroep digitaal forensisch onderzoeker. Deze specialisatie biedt de ICT-beheerder en Netwerk- en mediabeheerder meer kansen op de arbeidsmarkt. Daarnaast biedt het een oriëntatie op de doorstroommogelijkheid naar het hbo (Network Forensics Research).

Beschrijving van het keuzedeel

Het keuzedeel gaat in op het inventariseren van digitale sporen en het veiligstellen van onderzoeksmateriaal. Ook het verwerken en uitvoeren van onderzoek op onderzoeksmateriaal komt aan bod. Het preventief handelen staat centraal.

Branchevereisten

Nee

Aard van keuzedeel

Verdiepend

Doorstroom

2. Uitwerking

D1-K1: Inventariseren van digitale sporen en veiligstellen van digitaal onderzoeksmateriaal

Complexiteit

De beginnend beroepsbeoefenaar hanteert een gestructureerde werkwijze bij het inventariseren van digitale sporen en veiligstellen van digitaal onderzoeksmateriaal waarbij standaardwerkwijzen gelden. Zijn fysieke werkomgeving is in de meeste gevallen lokaal, hoewel zijn werk inhoudelijk op internationaal vlak kan begeven. Een complicerende factor is de verscheidenheid in zijn werk: het werken in verschillende situaties, uiteenlopende organisaties, digitale middelen en onderzoeksmaterialen en veranderende methodieken. Hij dient daarom te beschikken over specialistische kennis en vaardigheden op het gebied van het inventariseren van digitale sporen en het veiligstellen van digitaal onderzoeksmateriaal en bij zijn werkzaamheden in voorkomende gevallen de Engelse taal toe te passen.

Verantwoordelijkheid en zelfstandigheid

De beginnend beroepsbeoefenaar voert bij het inventariseren van digitale sporen en het veiligstellen van digitaal onderzoeksmateriaal zijn werkzaamheden veelal zelfstandig uit en is meestal verantwoordelijk voor een deelproces. Hierbinnen draagt hij verantwoordelijkheid voor eigen activiteiten, die op een forensische en juridische verantwoorde manier moeten verlopen en volgens beginselen van subsidiariteit en proportionaliteit. Hij krijgt zijn opdracht voor het inventariseren van digitale sporen en het veiligstellen van digitaal onderzoeksmateriaal meestal van een interne opdrachtgever, denk aan een security officer of een projectmanager. Bij de uitvoering van grotere opdrachten dient hij in teamverband te werken. Indien nodig roept hij de hulp in van interne of externe deskundigen.

Vakkennis en vaardigheden

De beginnend beroepsbeoefenaar:

- Heeft specialistische kennis over typen en soorten malware en spyware intrusions
- Heeft specialistische kennis van beginselen van subsidiariteit en proportionaliteit
- Heeft specialistische kennis van wetgeving relevant bij het inventariseren van digitale sporen en veiligstellen van digitaal onderzoeksmateriaal
- Heeft specialistische kennis van forensische en juridische procedures bij het veilig stellen van digitale sporen
- Kan specialistische kennis van de functies en mogelijkheden van software voor het inventariseren van digitale sporen en veiligstellen van digitaal onderzoeksmateriaal toepassen
- Kan brede kennis over typen en structuren systeemsoftware toepassen bij het verwerken en uitvoeren van onderzoek op onderzoeksmateriaal
- Kan specialistische kennis over internet resources en tools (bijv. way back machine) toepassen bij het verwerken en uitvoeren van onderzoek op onderzoeksmateriaal
- Kan ict en data methoden en technieken toepassen bij het inventariseren van digitale sporen en veiligstellen van digitaal onderzoeksmateriaal

D1-K1-W1: Selecteren van relevante digitale sporen

Omschrijving

De beginnend beroepsbeoefenaar bestudeert de onderzoeksvraag/opdracht. Hij inventariseert het aangeleverde digitale onderzoeksmateriaal. Hij bepaalt per type databron (b.v. data van computer of laptop, data van surfgedrag, emailverkeer, telefoonverkeer, GSM, PDA) hoe hij de benodigde sporen kan vinden. Hij controleert de verzamelde gegevens op integriteit (actualiteit en correctheid). Hij selecteert de data die relevant zijn voor het onderzoek.

Resultaat

Relevante digitale sporen zijn volgens de onderzoeksvraag c.q. opdracht geselecteerd.

Gedrag

De beginnend beroepsbeoefenaar

- houdt zich bij het selecteren van relevante digitale sporen aan wettelijke en voorgeschreven procedures.
- zet vakdeskundigheid in bij bepalen van juiste wijze om sporen te vinden.
- toont bij het selecteren van relevante data inzicht in mogelijke gevolgen voor het onderzoek.
- stelt zich integer op bij het werken met gevoelige informatie.

D1-K1-W1: Selecteren van relevante digitale sporen

De onderliggende competenties zijn: Ethisch en integer handelen, Instructies en procedures opvolgen, Vakdeskundigheid toepassen

D1-K1-W2: Veiligstellen van digitale sporen

Omschrijving

De beginnend beroepsbeoefenaar stelt de digitale sporen op een forensisch en juridisch verantwoorde wijze veilig. Daarbij gebruikt hij specifieke hard- en software om ervoor te zorgen dat bijvoorbeeld digitale opslagmedia niet meer beschreven kunnen worden, en hij maakt een forensisch verantwoorde kopie van het geselecteerde onderzoeksmateriaal zoals dit op dat moment is.

De beginnend beroepsbeoefenaar bepaalt per onderzoek of hij over de juiste kennis en/of middelen beschikt om de digitale sporen veilig te stellen. Zo nodig roept hij de hulp van interne of externe deskundigen in en waar nodig raadpleegt hij openbare bronnen.

Resultaat

Digitale sporen zijn volgens de voorgeschreven procedures veiliggesteld.

Gedrag

De beginnend beroepsbeoefenaar

- beslist tijdig of hij over de juiste kennis beschikt om digitale sporen veilig te stellen.
- roept tijdig de hulp in van interne of externe deskundigen.
- zet vakdeskundigheid in bij de keuze van relevante hard- en software, juiste tooling en wijze van veiligstellen.
- houdt zich bij het veiligstellen van digitale sporen aan wettelijke en voorgeschreven procedures.

De onderliggende competenties zijn: Beslissen en activiteiten initiëren, Samenwerken en overleggen, Materialen en middelen inzetten, Instructies en procedures opvolgen

D1-K2: Verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal

Complexiteit

De beginnend beroepsbeoefenaar hanteert een gestructureerde werkwijze bij het verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal waarbij standaardwerkwijzen gelden. Zijn fysieke werkomgeving is in de meeste gevallen lokaal, hoewel zijn werk inhoudelijk op internationaal vlak kan gebeven. Een complicerende factor is de verscheidenheid in zijn werk: het werken in verschillende situaties, uiteenlopende organisaties, digitale middelen en onderzoeksmaterialen en veranderende methodieken. Hij dient daarom te beschikken over specialistische kennis en vaardigheden op het gebied van het verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal en bij zijn werkzaamheden in voorkomende gevallen de Engelse taal toe te passen.

Verantwoordelijkheid en zelfstandigheid

De beginnend beroepsbeoefenaar voert bij het verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal zijn werkzaamheden veelal zelfstandig uit en is meestal verantwoordelijk voor een deelproces. Hierbinnen draagt hij verantwoordelijkheid voor eigen activiteiten, die op een forensische en juridische verantwoorde manier moeten verlopen en volgens beginselen van subsidiariteit en proportionaliteit. Hij krijgt zijn opdracht voor het verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal meestal van een interne opdrachtgever, denk aan een security officer of een projectmanager. Bij de uitvoering van grotere opdrachten dient hij in teamverband te werken. Indien nodig roept hij de hulp in van interne of externe deskundigen.

Vakkennis en vaardigheden

De beginnend beroepsbeoefenaar:

- Heeft specialistische kennis van de typering en eigenschappen van bronnen
- Heeft specialistische kennis van forensische en juridische procedures bij het verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal
- Heeft specialistische kennis van forensische middelen en methodieken voor het analyseren van digitaal onderzoeksmateriaal
- Heeft specialistische kennis van juridische wetgeving voor het verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal
- Heeft specialistische kennis van kwaliteitsnormen
- Heeft specialistische kennis van privacy wetgeving
- Heeft specialistische kennis van formats voor het leveren van input bij het maken van een onderzoeksrapport

- Kan analysemethoden toepassen bij het verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal
- Kan basispresentatietechnieken in de Nederlandse en Engelse taal toepassen bij de presentatie aan relevante betrokkenen
- Kan specialistische kennis van de functies en mogelijkheden van software voor het verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal toepassen
- Kan statistische methodes toepassen relevant bij het verwerken en uitvoeren van (deel)onderzoek op onderzoeksmateriaal

D1-K2-W1: Analyseren van veiliggestelde digitale sporen

Omschrijving

De beginnend beroepsbeoefenaar analyseert het veiliggestelde digitale onderzoeksmateriaal met behulp van analyse- en correlatietechnieken en maakt selectief gebruik van andere onderzoeksmiddelen. Hij bepaalt welke forensisch verantwoorde middelen en/of methodieken gehanteerd moeten worden. Naar aanleiding van de analyse legt hij de veiliggestelde digitale sporen vast en ordent hij deze volgens het format van het softwarepakket dat hij hiervoor gebruikt. Hij trekt conclusie met betrekking tot de analyse.

Resultaat

De veiliggestelde digitaliseerde sporen zijn geanalyseerd en zijn vastgelegd en geordend volgens het gedefinieerde format.

Gedrag

De beginnend beroepsbeoefenaar

- toont bij het analyseren van veiliggestelde digitale sporen inzicht in mogelijke gevolgen van zijn handelen voor de belangen van het bedrijf, de opdrachtgever of de privacy van personen.
- zet de middelen en methodieken doeltreffend in bij de analyse van digitale sporen.
- legt waar mogelijk en nodig verbanden tussen gegevens en trekt conclusies die voldoen aan het subsidiariteits- en proportionaliteitsbeginsel.
- blijft productief werken in een stressvolle omgeving.

D1-K2-W1: Analyseren van veiliggestelde digitale sporen

- werkt conform voorgeschreven (wettelijke) procedures en richtlijnen.

De onderliggende competenties zijn: Ethisch en integer handelen, Materialen en middelen inzetten, Analyseren, Leren, Met druk en tegenslag omgaan, Instructies en procedures opvolgen

D1-K2-W2: Raadplegen van relevante aanvullende bronnen

Omschrijving

De beginnend beroepsbeoefenaar bepaalt welke aanvullende openbare en/of gesloten bronnen relevant zijn en bestudeerd moeten worden. Hij bestudeert deze bronnen en voegt de eventueel daar aangetroffen extra informatie toe aan het overige onderzoeksmateriaal.

Resultaat

Het onderzoeksmateriaal is completer geworden en voldoet aan vastgestelde en voorgeschreven kwaliteitsnormen.

Gedrag

De beginnend beroepsbeoefenaar

- zet vakdeskundigheid in bij het kritisch analyseren van de gevonden informatie op juistheid, relevantie en extra toegevoegde waarde op het onderzoeksmateriaal.
- onderzoekt bij het toevoegen van gevonden informatie aan het onderzoeksmateriaal op detailniveau grondig of hij correct te werk is gegaan.

De onderliggende competenties zijn: Analyseren, Kwaliteit leveren

D1-K2-W3: Leveren van input voor het maken van het onderzoeksrapport

Omschrijving

De beginnend beroepsbeoefenaar beschrijft in het logboek de gevolgde werkwijze en op basis van objectieve waarheidsvinding gevonden resultaten. Hij maakt een samenvatting en levert input aan het onderzoeksrapport. Hij beantwoordt vragen van de interne opdrachtgever en licht de samenvatting van het opgeleverde onderzoeksmateriaal toe aan relevante betrokkenen.

Resultaat

Werkwijze en resultaten zijn vastgelegd.
Een correcte samenvatting en presentatie van het opgeleverde onderzoeksmateriaal.
Een tevreden interne opdrachtgever en betrokkenen over de toelichting en bijdrage aan het onderzoeksrapport.

Gedrag

De beginnend beroepsbeoefenaar

- neemt een adequate beslissing over het bewaken van geheimhouding, zoals vertrouwelijkheid van gegevens en objectiviteit van aangeleverde input.
- structureert de informatie overzichtelijk en formuleert in correcte zinnen in de Nederlandse en Engelse taal.
- weet vragen over het opgeleverde onderzoeksmateriaal adequaat te beantwoorden.

De onderliggende competenties zijn: Ethisch en integer handelen, Formuleren en rapporteren, Op de behoeften en verwachtingen van de "klant" richten

D1-K2-W4: Afronden van het onderzoek

Omschrijving

De beginnend beroepsbeoefenaar rondt het onderzoek af. Hij ruimt materiaal en gereedschappen op en stelt deze veilig.

Resultaat

Zorgvuldig en ordelijk opgeruimd en veilig gesteld materiaal en gereedschappen.

Gedrag

De beginnend beroepsbeoefenaar

- werkt bij veiligstelling van het materiaal en gereedschappen nauwkeurig en volgens een systematische werkwijze.

De onderliggende competenties zijn: Vakdeskundigheid toepassen, Materialen en middelen inzetten