Exameneisen Proactief beveiligen

Toelichting
Voor alle exameneisen geldt dat waar gesproken wordt van kennis van de begrippen ook voorbeelden van deze begrippen kunnen worden gevraagd in een examen.

De commissie van deskundigen voor proactief beveiligen heeft ernaar gestreefd om zoveel mogelijk tot een gezamenlijke norm te komen. De inhoudelijke overeenstemming is tot stand gekomen door verschillen van inzicht en interpretatie, die logischerwijs ontstaan tussen deskundigen met een verschillende achtergrond, opzij te zetten. Daarnaast dicteert de praktijk de proactieve beveiligingsmethodiek en niet andersom, zodat ook aanpassingen en verbeteringen een continu proces blijven van kritische beschouwing.
Ter onderbouwing van de normen is ervoor gekozen om waar nodig exameneisen te voorzien van een toelichting. Deze teksten zijn cursief en in een kleiner lettertype weergegeven. Het is de taak van uitgeverijen, opleiders en vakdocenten om exameneisen uit te werken in cursusmateriaal en in een passend curriculum aan te bieden aan cursisten.

1. Introductie proactief beveiligen

1.01
Beschrijft de doelstelling van proactief beveiligen.
Proactief beveiligen is een vorm van beveiligen die zich richt op het actief detecteren van de voorbereidende stappen die voorafgaan aan voornamelijk terroristische en criminele acties. Bij ontdekking van mogelijke voorbereidingen kunnen er proactief extra veiligheidsmaatregelen worden getroffen zodat de beoogde uitvoering door de tegenstander(s) onmogelijk wordt gemaakt.

1.02
Beschrijft en onderscheidt de begrippen actieve en passieve maatregelen in relatie tot preventie.
Actieve maatregelen: hierbij gaat de proactieve beveiliger actief op zoek naar verdachte indicatoren bij personen, voorwerpen, situaties of informatie die een relatie hebben met een AMO. Als verdachte indicatoren worden ontdekt, worden deze onderzocht door middel van prikkelen en Security Questioning. Aan de hand van het SQ gesprek wordt er een dreigingsbeslissing genomen waarna de SOP wordt gevolgd en mogelijk aanvullende preventieve maatregelen kunnen worden genomen.
Passieve maatregelen: Elektronische en bouwkundige maatregelen.

1.03
Beschrijft het begrip proactief beveiligen.
Het uitvoeren van een dreigingsassessment ten aanzien van een persoon, voorwerp, situatie en informatie op basis van verdachte indicatoren in een relatie met een AMO.

1.04
Beschrijft en onderscheidt:
a. denken vanuit het perspectief van de tegenstander
   Om de tegenstander van het te beschermen gebied te ontdekken en daarna actief te ontmoedigen zodat hij zijn AMO niet langer kan/wil uitvoeren is het noodzakelijk dat de proactieve beveiliger de voorbereiding en uitvoeringstactieken kent van de mogelijke tegenstanders binnen zijn operationele omgeving.
b. in zo'n vroeg mogelijk stadium onderkennen van een dreiging door uitvoeren van een dreigingsassessment
   De bedoeling van het dreigingsassessment is een potentiële tegenstander zo vroeg mogelijk vanuit een aanvallende naar een verdedigende positie te brengen. Hierdoor wordt de rol van aanvaller en verdediger omgedraaid en ligt het initiatief weer bij de verdediger.
c. het op een juiste wijze handelen t.a.v. een onderkende dreiging
   De juiste wijze van handelen t.a.v. een dreiging zijn vastgelegd in de SOP. Hierin staan de door de organisatie gewenste handelingen die de proactieve beveiliger dient uit te voeren om zo de onderkende dreiging te stoppen. De SOP wordt door elke organisatie zelf ingericht en zijn dus per operationeel gebied anders.
   Het op een juiste wijze handelen in geval van een dreiging ligt vast in protocollen die van tevoren zijn afgestemd met het management van de organisatie. Acties om dreigingen te mitigeren hebben vaak impact op het primaire proces van de organisatie. Hier houdt de keuzevrijheid van de proactieve beveiliger op en handelt hij conform zijn SOP.

1.05
Beschrijft en onderscheidt de voorwaarden en competenties waaraan een proactieve beveiliger moet voldoen.
Voorwaarden:
- *bekend zijn met de te beschermen omgeving: wat moet er worden beveiligd*
- *bekend zijn met de operationele omgeving: hoe zit deze in elkaar, welke primaire processen zijn er. Wie zijn de vaste leveranciers en externe dienstverleners. Met welk doel komen mensen op bezoek. Wie werkt er waar binnen het te beveiligen object.*
- *bekend zijn met de norm van zijn omgeving: wat is normaal op verschillende momenten van de dag/week/maand*
- *bekend zijn met de dreigingen: wat zijn de dreigingen die de te beschermen omgeving bedreigen. Deze dreigingen komen uit de dreigingsanalyse. De dreigingsanalyse geeft antwoord op drie vragen:*
  - *wat moet er beschermd worden (te beschermen omgeving)*
  - *wie is geïnteresseerd in de te beschermen omgeving (potentiele tegenstanders)*
  - *hoe gaan mogelijke daders te werk om hun doel te bereiken? (AMO)*
- *bekend zijn met de AMO's: welke AMO's zijn in de dreigingsanalyse vastgesteld*
- *dreiging georiënteerd zijn*

Competenties:
- *kunnen observeren en waarnemen, oog hebben voor detail*
- *besluitvaardig zijn*
- *communicatief vaardig zijn, een gesprek kunnen voeren. Om dit te kunnen moet de proactieve beveiliger goed kunnen luisteren, brede interesse hebben voor de actualiteiten en algemene ontwikkeling.*
- *zelfvertrouwen hebben*

1.06
Beschrijft en onderscheidt tussen een risico en een dreiging.
Een risico is meetbaar en heeft niveaus (kans x effect). Dreiging is te koppelen aan een AMO en is niet meetbaar. Het hoeft nog niet eerder gebeurd te zijn. Dreiging gaat uit van de mogelijkheden van de tegenstander.

1.07
Beschrijft het te beschermen belang in relatie tot een operationele omgeving.
Het is voor de proactieve beveiliger belangrijk om te weten wat het te beschermen belang is en hoe een tegenstander daar in zijn operationele omgeving mogelijk toegang tot kan verkrijgen.

1.08
Beschrijft en onderscheidt de vier factoren van het NAVI-model die eraan kunnen bijdragen dat een dader zijn daad uitvoert.
Dit heeft betrekking op het 'willen' (motivatie) wat wordt bepaald door de mate van attractiviteit van het te beschermen belang en de kans op succes en het kennen van de dader wat wordt bepaald door de voldoende aanwezigheid van kennis en middelen.

1.09
Beschrijft en onderscheidt de volgende dadergroepen (volgens de NAVI-typering):
a. crimineel
b. medewerker
c. bezoeker
d. vandaal
e. hacker
f. activist
g. terrorist
h. verward persoon
De tegenstander bestaat uit verschillende dadertypen. De dadertypen worden vanuit de dreigingsanalyse onderkend. Het doel en werkwijze verschilt per dadertype. De medewerker en bezoeker staan ertussen vanwege de legitimatie van aanwezigheid tot het te beschermen belang en kunnen met een kwade intentie acties uitvoeren.

2. Criminele/terroristische planningscyclus

2.01
Beschrijft en onderscheidt de acht stappen die een crimineel of terrorist doorloopt om zijn doel te bereiken.
1. *selecteert doel(en)*
2. *verzamelt informatie*
3. *surveilleert*
4. *plant aanval*
5. *verzamelt middelen*
6. *oefent / dry run*
7. *voert uit*
8. *vlucht*

2.02
Plaatst waarnemingen in de criminele planningscyclus.
Het doel van deze eis is om het onderscheid te maken tussen voorbereidende AMO's en uitvoerende AMO's. Het is voor de proactieve beveiliger veilig om contact te maken als het voorbereidende handelingen betreft (stap 2 en 3).

2.03
Beschrijft het begrip social engineering.
Door misleiding een persoon dingen laten doen die hij onder normale omstandigheden nooit zou doen voor een vreemde of buitenstaander met als gevolg schade voor de persoon of groter voor zijn werkgever. Social engineering kan zowel via de digitale weg worden toegepast (internet, social media, e-mails etc.), maar ook in real life door m.b.v. een cover en bijpassende coverstory toegang te verkrijgen tot bijvoorbeeld gevoelige informatie.
In de praktijk worden social engineering tactieken uitgevoerd door het opwekken van nieuwsgierigheid, intimidatie, gebruik maken van standaardroutines of onze natuurlijke neiging om behulpzaam te zijn.

3. Aanvallers Methode van Operatie (AMO)

3.01
Beschrijft het begrip AMO en onderscheidt de twee typen. Beschrijft hoe men tot een AMO komt.
AMO staat voor Aanvallers Methode van Operatie. Een AMO is een wijze van werken waarvan in de praktijk is bewezen dat deze daadwerkelijk uitvoerbaar is. De twee typen zijn voorbereidende AMO's en uitvoerende AMO's.

3.02
Beschrijft de afkorting KISS. Licht de relatie tot de AMO toe.
Keep It Smart and Simple. Een dader zal bij voorkeur kiezen voor een AMO die makkelijk uit te voeren is. Een te complex AMO verhoogt de kans op falen of vroegtijdige ontdekking.

3.03
Beschrijft en onderscheidt de begrippen deels naïeve en naïeve persoon.
Het betreft hier het verschil tussen het wel of niet hebben van een slechte intentie.
- *deels naïef: persoon denkt iets te gaat doen waarmee hij de wet overtreedt (crimineel), echter blijkt dit tijdens de uitvoering zonder zijn medeweten van terroristische aard te zijn*
- *naïef of mule (Engels voor ezel): persoon weet niet dat hij onderdeel is van een terroristische (of criminele) actie, maar is wel een belangrijk onderdeel van de uitvoering. Deze laatste zal voor de proactieve beveiliger lastig te detecteren zijn aangezien er geen zichtbare verdachte gedragsindicatoren zijn*

4. Verdachte indicatoren

4.01
Beschrijft en onderscheidt de begrippen verdachte indicator en normale situatie.
Een verdachte indicator is een zichtbare aan AMO te koppelen afwijking van de norm. Verdachte indicatoren zijn tijd, plaats en cultuurafhankelijk en daarmee vormen zij een contrast met een normale situatie of omgeving context. Om de norm van een te beschermen belang te kunnen vaststellen zal de proactieve beveiliger een beeld moeten krijgen bij wat 'normaal' is voor die omgeving. Wie houdt zich normaliter op in deze omgeving, hoe deze personen zich gedragen, waarom ze in deze omgeving zijn, wat ze bij zich hebben en met welke intentie ze daar zijn. De norm is voor een bepaalde omgeving niet altijd hetzelfde. Zo geldt er bijvoorbeeld een andere norm voor de omgeving voor openingstijd, tijdens openingstijd en na openingstijd. Ook kunnen tijdelijke andere activiteiten invloed hebben op de norm die op dat moment geld voor de omgeving. Tijdens een bedrijfsfeestje zal de norm anders zijn dan tijdens normale werktijden. Normaal is datgene wat door de meeste mensen geaccepteerd wordt of dat wat de meeste mensen doen. Het wijkt niet af van de gangbare praktijk, ofwel iets verloopt volgens de regel.

4.02
Beschrijft van welke factoren een normale situatie afhankelijk is.
De norm is dynamisch en is tijd, plaats en cultuur afhankelijk.

4.03
Beschrijft uit welke aandachtsgebieden verdachte indicatoren kunnen ontstaan.
- *gedrag*
- *uiterlijk voorkomen niet zijnde etnische afkomst of anderszins*
- *bezittingen*
- *het verhaal dat iemand vertelt*
- *documentatie*
- *de situatie*

4.04
Beschrijft wanneer iemand vreemd gedrag vertoont aan de hand van een gegeven norm.
- *verdacht gedrag: als er een relatie is tussen specifieke verdachte indicatoren en een specifieke werkwijze van een tegenstander, ook wel aanvallers modus van operandi genoemd (AMO)*
- *vreemd gedrag: een afwijking van wat normaal is voor een bepaalde omgeving, maar zijn geen verdachte indicatoren die te koppelen zijn aan een AMO*
- *normaal gedrag: het gedrag past in de omgeving en bij de norm die geldt voor die specifieke omgeving*

4.05
Beschrijft en onderscheidt de drie elementen van een goede coverstory. Licht toe wat de taak van de proactieve beveiliger hierbij is.
Een goede coverstory bestaat uit drie elementen: een cover voor de identiteit, een cover voor het tijdstip en de locatie en een cover voor de missie. De taak van de proactieve beveiliger is het herkennen en doorbreken van een cover en de coverstory als daar sprake van is.

4.06
Beschrijft en onderscheidt verdachte indicatoren in relatie tot het verifiëren van Nederlandse identiteitsbewijzen.
- *persoon spreekt niet de taal van zijn ID*
- *persoon weet te weinig of juist te veel details van zijn ID*
- *kenmerken van de persoon zoals leeftijd, lengte, geboortedatum komen niet overeen met de persoon die voor je staat*
- *ID lijkt aangepast of veranderd*
- *persoon probeert zijn gezichtskenmerken te verbergen tijdens SQ interview*

4.07
Beschrijft het begrip aanname. Licht toe wat de taak van de proactieve beveiliger hierbij is.
Een proactieve beveiliger wil zoveel mogelijk zeker weten en moet voorbij de schijn der dingen kunnen kijken, denken en vragen.

5. Security Questioning(SQ)

5.01
Beschrijft en onderscheidt de doelen van Security Questioning. Beschrijft en onderscheidt SQ-vragen.
Hierbij moet bekend zijn dat er geen standaard SQ vragen zijn. Dit zou SQ voorspelbaar maken ten voordele van een tegenstander die deze vragen kan voorbereiden.

- *ontdekken van meerdere verdachte indicatoren: tijdens het uitvoeren van de Security Questioning zal de proactieve beveiliger alert moeten zijn op mogelijke bijkomende verdachte indicatoren die tijdens het gesprek ontstaan*
- *weerleggen van de verdachte indicatoren: met het weerleggen van de verdachte indicatoren wordt bedoeld dat de proactieve beveiliger op zoek gaat tijdens het Security Questioning gesprek naar een logische verklaring voor de verdachte indicatoren die zijn gezien. Is er een logische verklaring te vinden dat het gedrag of wat de persoon bij zich heeft te verklaren wat ontkracht dat deze een slechte intentie heeft?*
- *ontdekken wat de intentie is: in het gesprek wordt de intentie van de persoon gevraagd en bevraagd. Wat is de persoon van plan, waarom is hij hier en wat gaat de persoon straks doen?*
- *vaststellen wat het AMO is: als de verdachte indicatoren niet opgelost kunnen worden zal de proactieve beveiliger proberen te kijken welk mogelijk AMO er van toepassing is. Dit is niet altijd mogelijk omdat sommige verdachte indicatoren kunnen wijzen op meerdere AMO's. Er wordt dan altijd uitgaan van het AMO die de grootste schade zal veroorzaken. De tegenmaatregelen zullen hierop zijn gebaseerd.*
- *ontdekken van een eventuele cover story: tijdens het gesprek wordt onderzocht of er sprake is van een cover en coverstory*
- *verzamelen van informatie: in het gesprek wordt zoveel mogelijk informatie verzameld door middel van de vragen, in een zeer korte tijd. Deze informatie kan namelijk helpen bij het verscherpen van de verdachte indicatoren en als er een dreiging blijkt om deze op basis van die informatie af te zwakken.*
- *afschrikken: algemeen doel van Security Questioning is het prikkelen van de tegenstander en het gevoel geven dat deze is gezien en zijn intentie is ontdekt. Hierdoor zullen er onafhankelijkheden in de vorm van tegenmaatregelen worden genomen zodat zijn plan geen succes meer zal behalen. Het is echter niet de bedoeling dat de personen die gewenst of geaccepteerd zijn in het te beschermen gebied last hebben van Security Questioning. De wijze van bevragen dient daarom altijd vriendelijk, servicegericht, discreet en oprecht geïnteresseerd te zijn.*

5.02
Beschrijft waarom het een crimineel/terrorist kan afschrikken als hem door een persoon vragen worden gesteld.
Tijdens het stellen van vragen worden de rollen van verdediger en aanvaller omgedraaid. De aanvaller moet in de verdediging en gaan improviseren onder druk. Dit zal ervoor zorgen dat de aanvaller problemen gaat krijgen om zijn houding en gedrag natuurlijk te laten overkomen.

5.03
Beschrijft en onderscheidt de begrippen Security Questioning en een (politie)verhoor.
Security Questioning heeft een andere manier van werken en benadering dan een verhoor. De belangrijkste verschillen zijn:

Security Questioning	*Verhoor*
▪ *zoeken naar de intentie*	▪ *zoeken naar de middelen*
▪ *verificatie*	▪ *bewijs verzamelen*
▪ *ontkrachten van de dreiging*	▪ *beschuldigend van toon*
▪ *coöperatief van toon*	▪ *autoritaire houding*

Een proactieve beveiliger voert zijn Security Questioning gesprek met een persoon altijd op basis van vrijwilligheid. Dit is de reden dat een proactieve beveiliger voor aanvang van het gesprek altijd eerst toestemming vraagt en een onderbouwing geeft waarom een gesprek gewenst is. De politie eist dat de persoon meewerkt aan het gesprek in de vorm van een verhoor. Security Questioning mag nooit worden ervaren als een verhoor. Er is tenslotte geen zekerheid of de persoon met wie het gesprek wordt gevoerd inderdaad een tegenstander is of een bezoeker/gast/medewerker etc. In tegenstelling tot een verhoor zal een proactieve beveiliger ook nooit een bekentenis krijgen van zijn tegenstander, dus zoekt er ook niet naar.

5.04
Beschrijft en onderscheidt de kenmerken van Security Questioning.
a. er is sprake van beperkte tijd
Er moet snel een dreiging geen dreigingsbeslissing worden gemaakt waarbij de proactieve beveiliger het moet doen met beperkte informatie.
b. er is geen hiërarchische verhouding tussen de proactieve beveiliger en de persoon waarbij SQ wordt uitgevoerd
SQ is altijd op basis van vrijwilligheid. De persoon in kwestie moet ook nadrukkelijk om toestemming worden gevraagd en weten waarom er vragen worden gesteld.
c. SQ is flexibel en niet geautomatiseerd
Vragen en doorvragen is altijd op basis van de antwoorden die worden gegeven dit kan dus per definitie niet worden geautomatiseerd.
d. SQ is gedreven door de werkwijze van de tegenstander
SQ vragen richten zich op het ontkrachten van de verdachte indicatoren en daarmee op de werkwijze van de tegenstander.

5.05
Beschrijft en onderscheidt de stappen van het proces van Security Questioning
a. initiële indruk / eerste indruk
Houding, gedrag, verdachte indicatoren, is de persoon alleen of met anderen, wat heeft de persoon bij zich aan bagage, waar komt te persoon vandaan?
b. contact maken met de persoon
Professionele introductie van de proactieve beveiliger: Goede…mijn naam is…. Ik ben beveiliger bij…. Ik zou u graag een paar vragen willen stellen die te maken hebben met uw en onze veiligheid, vindt u dat goed?
c. gesprek voeren
Vragen en doorvragen waarbij de proactieve beveiliger de regie heeft en behoudt. Doel is om zo snel mogelijk alle verdachte indicatoren te ontkrachten.
d. gesprek afsluiten
Professionele afsluiting: Hartelijk dank voor uw medewerking ik wens u nog een fijne dag. Ook in het geval van dreiging op dezelfde manier afsluiten tenzij de persoon in kwestie de toegang wordt geweigerd of alsnog wordt ontzegd.
De uitkomsten van het dreigingsassessment na Security Questioning zijn:
- *ontkrachte dreiging: de proactieve beveiliger heeft de verklaring gekregen voor de verdachte indicatoren. De vervolgacties zijn (afhankelijk van het te beveiligen object) vastgelegd in zijn SOP.*
- *dreiging: de proactieve beveiliger voert de acties uit zoals vastgelegd in zijn SOP*

5.06
Beschrijft hoe een proactieve beveiliger tijdens Security Questioning om dient te gaan met verborgen verdachte indicatoren.
Tijdens SQ probeert de proactieve beveiliger bij voorkeur de verdachte indicatoren te ontkrachten zonder deze te benoemen tijdens SQ. Als er tijdens het gesprek nieuwe verdachte indicatoren worden ontdekt zal de proactieve beveiliger hier ook vragen over moeten stellen om deze te proberen te ontkrachten.

5.07
Beschrijft en onderscheidt gesloten en open vragen. Beschrijft waar tijdens Security Questioning meestal de voorkeur naar uitgaat.
De voorkeur gaat uit naar korte open vragen omdat deze vragen meer informatie geven aan de proactieve beveiliger. Gesloten vragen kenmerken zich door het feit dat deze met ja of nee kunnen worden beantwoord.

5.08
Beschrijft welke signalen tijdens Security Questioning kunnen duiden op liegen.

- *aarzelen met antwoord geven*
- *gedetailleerde respons versus korte en algemene respons*
- *proberen van onderwerp te veranderen*
- *vragen beantwoorden met vragen*
- *te coöperatief*
- *incoherent verhaal*
- *veranderingen in lichaamstaal*
- *babbelen*
- *fysieke signalen van liegen zoals bijvoorbeeld micro expressies welke de ware emotie onder stress laten zien.*

5.09
Beschrijft voor een gegeven situatie welke indicatoren er zijn voor een cover.

6. Dreigingsassessment

6.01.01
Beschrijft het begrip dreigingsassessment.
Proactief beveiligen is het uitvoeren van een dreigingsassement ten aanzien van een persoon, voorwerp, of situatie op basis van normafwijkingen in een relatie met een AMO.
Een dreigingsassessment is het vaststellen of er ten aanzien van normafwijkingen in relatie met een AMO (verdachte indicatoren) een dreiging uitgaat.

6.01.02
Beschrijft en onderscheidt de stappen van het dreigingsassessment.
a. detecteren van de afwijking van de norm
b. beslissen of de afwijking gekoppeld kan worden aan een AMO
c. door middel van SQ zoeken naar een verklaring voor de verdachte indicator
d. beslissen wat de uitkomst is van het gesprek: wel of geen dreiging

6.02.01
Beschrijft het begrip classificatie.
De proactieve beveiliger classificeert de indicatoren die worden waargenomen of aan hem worden doorgegeven door anderen. Classificeren betekent dat hij een afweging maakt of er mogelijk sprake is van een verdachte indicator. Na het voeren van een Security Questioning gesprek of servicegesprek zal de proactieve beveiliger deze afweging opnieuw maken om tot een dreigingsbeslissing te komen. De classificatie van de indicatoren staan genoemd in de SOP gekoppeld aan AMO's en gewenste opvolgingsacties.
Deze niveaus zijn in de praktijk meestal:
- *geen verdachte indicator*
- *verdachte indicator*
- *ontkrachte verdachte indicator*
- *niet ontkrachte indicator*

6.02.02
Beschrijft en onderscheidt de classificaties die kunnen voortkomen uit een dreigingsassessment.
Een verdachte indicator is een waargenomen normafwijking gekoppeld aan een AMO. Deze is waargenomen, dus de verdachte indicator is er. Echter een verdachte indicator hoeft geen dreiging te zijn. Na SQ blijkt of er wel of geen sprake is van een dreiging. De uitkomst van SQ is dus:
a. dreiging: geen verklaring gekregen voor de verdachte indicatoren
b. ontkrachte dreiging: er is een verklaring gekregen voor de verdachte indicatoren waardoor de dreiging is ontkracht
c. van geen dreiging is sprake indien de normafwijking niet gerelateerd kan worden aan een AMO

6.03
Beschrijft aan de hand van een gegeven situatie of een afwijking gekoppeld kan worden aan een AMO waardoor er sprake is van een verdachte indicator.

6.04
Beschrijft aan de hand van een gegeven situatie of er sprake is van een dreiging.

7. Standaard operationele procedures (SOP)

7.01
Beschrijft en onderscheidt de onderdelen van een SOP.
1. operationele omgeving
Voor welk deel van het te beschermen gebied is de SOP van toepassing.
2. risicopositie
Voor welke risicopositie zijnde betreffende AMO's en verdachte indicatoren van toepassing.
3. AMO's
Met welke AMO's staat de aangegeven verdachte indicator mogelijk in relatie.
4. verdachte indicatoren (VI)
Wat zijn de verdachte indicatoren die van toepassing zijn op een bepaalde risicopositie
5. classificaties t.b.v. de vervolgacties
Welke classificaties kunnen worden toegekend na het uitvoeren van het dreigingsassessment.
6. vervolgacties per classificatie
Wat zijn de exacte vervolgacties nadat er een classificatie is toegekend.

7.02
Beschrijft en onderscheidt de soorten AMO's die in een SOP worden weergegeven. Koppelt dit aan de eigen veiligheid.
Voorbereidende en uitvoerende AMO's: deze zijn te relateren aan de voorbereidende stappen informatie verzamelen en surveillance uit de criminele/terroristische planningscyclus.

8. Red teaming

8.1
Beschrijft het begrip Red Teaming en geeft aan wat het doel is.
Het vanuit een onafhankelijke positie uitvoeren van een gecoördineerde aanval met als doel de bestaande aannames en bestaande beveiligingsmaatregelen te testen. Met Red teaming kunnen nieuwe AMO's worden ontdekt of bestaande AMO's worden getest.

8.2
Beschrijft en onderscheidt interne en externe Red Teaming met betrekking tot uitvoering en doel.
Interne Red Teaming wordt uitgevoerd in opdracht van de leidinggevende door proactieve beveiligers in de eigen organisatie met als doel de proactieve beveiligers te laten ervaren wat een slechte intentie doet met het eigen gedrag. Hoe gaan zij zelf afwijken van de norm. Daarnaast kan het doel zijn om mogelijke nieuwe AMO's te testen of extra awareness bij andere afdelingen te realiseren.
Externe Red Teaming wordt uitgevoerd door een Red Team dat bestaat uit personen die niet werkzaam zijn in de organisatie waarbij geredteamt gaat worden. Deze personen staan echter wel onder leiding van iemand uit deze organisatie op afstand. Externe Red Teaming wordt nooit uitgevoerd zonder opdracht en toestemming van de hoogst verantwoordelijke in de betreffende organisatie en onder strikte geheimhouding. Doel van externe Red Teaming is nieuwe en bestaande AMO's te kunnen testen en kunnen ook als oefening worden aangeboden aan proactieve beveiligers om in hun eigen werkomgeving te kunnen oefenen met verdachte indicatoren en SQ.

8.3
Beschrijft en onderscheidt de stappen bij het organiseren van Red Teaming.
a. bepalen van het doel van de oefening
Voor elke Red Teaming oefening wordt vooraf door de leidinggevende van de beveiliging aangegeven welk AMO en met welke spelregels de oefening uitgevoerd moet worden.
b. verkrijgen van de benodigde middelen
Door het scenario voor te laten bereiden en verder uit te laten werken door het Red Team kunnen zij aangeven welke middelen zij nodig denken te hebben om de oefening uit te kunnen voeren. Na goedkeuring van het scenario door de leidinggevende kan ook toestemming worden gegeven voor het organiseren van de benodigde middelen.
c. regelen van de coördinatie en supervisie
Voor, tijdens en na de oefening is er altijd een white team verantwoordelijk voor de coördinatie en toezicht op de oefening. Dit team kan uit een of meerdere personen bestaan en onderhoudt het contact met de leidinggevende en met het Red Team. Het white team kan ten alle tijden hierdoor de oefening bijsturen of stoppen als dit gewenst is (bijvoorbeeld in geval van een echte dreiging of calamiteit).
d. briefing en debriefing
Het zogenaamde white team zorgt voor de briefing en debriefing van het Red Team voor en na de oefening. Tijdens de briefing wordt het scenario en de spelregels nogmaals doorgenomen met het Red Team en de communicatie tijdens de oefening duidelijk vastgesteld. Dit is een voorwaarde voor mogelijke bijsturing tijdens de oefening en indien de oefening onverwachts afgebroken moet worden. Tijdens de debriefing hoort het white team het red team uit en legt de ervaringen, observaties en resultaten vast en verwerkt deze in een rapportage.
e. beoordelen en rapportage van de oefening
Het white team zorgt ervoor dat de resultaten van de oefening direct worden verwerkt in een rapportage en vult deze aan met materiaal dat mogelijk tijdens de oefening is verzameld (video- en/of audiobeelden, chatgeschiedenis mobiele apps etc.) en draagt deze over aan de leidinggevende die verantwoordelijk is voor de Red Teaming. Deze zal de oefening beoordelen op basis van:
- *nieuwe kwetsbaarheden ontdekt ja/nee*
- *nieuw AMO / bestaand AMO uitvoerbaar ja/nee*

Als nieuwe kwetsbaarheden worden ontdekt dan wordt er gekeken hoe deze strategisch gedicht kunnen worden. Bijvoorbeeld door coaching/training (bij persoon), updates/aanpassingen (elektronisch), extra borging/versteviging (bouwkundig).