Bijlage 3 - RVICTO 26 marktraadpleging | concept Programma van Eisen
Red teaming

Specifieke eisen Red teaming

Dit hoofdstuk bevat specifieke eisen die van toepassing zijn op Red Teaming testen. De Red Teaming testen worden in beginsel uitgevoerd volgens het TIBER-rijk of ART-rijk raamwerk en begeleid door het TCT-rijk.

In de kolom wordt aangeven of een eis van toepassing is voor TIBER, ART of beiden. (ART is modulair van opzet dus niet elke eis is van toepassing).

NB: Voor het uitvoeren van een TIBER-rijk of ART-rijk Red teaming test is betrokkenheid van het TCT-Rijk essentieel. Het TCT-rijk heeft een adviserende- en kwaliteitsbewakingsrol.

Indien een Red teaming dienst/opdracht niet (volledig) wordt uitgevoerd volgens het TIBER- of ART-raamwerk (Rijk), dan gelden in beginsel alle eisen die van toepassing zijn op het ART-raamwerk, met uitzondering van de eisen die gezien de door de Deelnemer vermelde uitzonderingen op het ART-raamwerk niet van toepassing kunnen zijn op deze opdracht. Een Deelnemer geeft bij voorkeur deze uitzonderingen in zijn aanvraag richting Opdrachtnemers aan.

In dit hoofdstuk zijn alleen de specifieke eisen voor het daadwerkelijke Red teaming Opdracht opgenomen. Eisen t.a.v. de Threat Intelligence opdracht (welke aan de RT voorafgaat) zijn/worden niet opgenomen. De RT-provider ontvangt voor aanvang werkzaamheden het TI-rapport van Deelnemer.

Basiseisen *Dit gedeelte omvat eisen van algemene aard aangaande het leveren van Red teaming diensten.*		**ART**	**TIBER**
B3.1	Bij uitvoering van de opdracht houdt Opdrachtnemer zich aan *NOK bijlage xx -de ethical standards of hacking*.	X	X
B3.2	De Opdrachtnemer voert de opdracht uit conform *NOK bijlage xx - het (concept) ART-rijk raamwerk (guidance documents)* die door Deelnemer, namens het Test Control Team (TCT) Rijk worden verstrekt. Zie de bijlage voor een actuele versie. TCT kan opvolgende versies vaststellen, waar Opdrachtnemer zich dan aan houdt.	X	
B3.3	De Opdrachtnemer voert de opdracht uit conform het *NOK bijlage xx - (concept) TIBER-rijk raamwerk (guidance documents)* die door de Deelnemer, namens het Test Control Team (TCT) Rijk worden verstrekt. Zie bijlage voor een actuele versie. TCT kan opvolgende versies vaststellen, waar Opdrachtnemer zich dan aan houdt.		X
B3.4	De Opdrachtnemer communiceert conform operationele werkafspraken die door het control team van Deelnemer zijn opgesteld.	X	X
B3.5	Opdrachtnemer komt bij uitvoering van de Opdracht in aanraking met bijzondere (gerubriceerde) informatie die valt onder het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIRBI) 2013 of gevoelige informatie die volgens Deelnemer een vergelijkbaar niveau van veiligheidsclassificatie krijgen. De Opdracht en de daaruit voortvloeiende documentatie en rapportages dienen te worden gerubriceerd als (minimaal) departementaal vertrouwelijk. De Deelnemer kan te allen tijde de classificering/rubricering verhogen indien zij daar noodzaak toe ziet. Opdrachtnemer houdt hij zich aan de toepasselijke bindende voorschriften/voorwaarden die Deelnemer of een door Deelnemer aangewezen beveiligingsautoriteit hieraan stelt. Opdrachtnemer dient alle (gerubriceerde) data en documenten, rapportages etc. met betrekking tot de Opdracht(en) o.a. versleuteld en beveiligd op te slaan. De integriteit van alle testresultaten is gewaarborgd. Voor de maatregelen van veilige uitwisseling van gerubriceerde of gevoelige informatie zullen Deelnemer en Opdrachtnemer nadere (bindende) voorwaarden overeenkomen.	X	X
B3.6	De Opdrachtnemer zorgt dat de gevolgen van de tests geen blijvende schade achterlaten en dat deze teruggedraaid kunnen worden dan wel op andere wijze worden hersteld. Hierbij gaat het bijvoorbeeld ook om het opruimen van (onwenselijke) sporen die tijdens de aanval zijn achtergebleven.	X	X

B3.7	Opdrachtnemer, Deelnemer en eventueel nog derden (voor zover te onderzoeken objecten niet in eigendom van Deelnemer zijn) komen per Nadere overeenkomst een vrijwaringsverklaring overeen voor het uitvoeren van de opdracht**.** *Partijen kunnen hierbij gebruikmaken van het model in bijlage xx.* In de vrijwaringsverklaring worden de risico's beschreven die het uitvoeren van het onderzoek met zich meebrengt, wordt toestemming gegeven voor aanval op toegang tot bepaalde objecten en wordt vrijwaring van aansprakelijkheid met betrekking tot de uitvoering van het onderzoek nader geregeld. De Deelnemer draagt zorg voor afstemming met eventuele derden en ondertekening en retournering van de vrijwaringsverklaring aan opdrachtnemer voordat het onderzoek start. Een door bevoegde functionaris(sen) ondertekende vrijwaringsverklaring wordt dan onderdeel van de betreffende Nadere overeenkomst. Opdrachtnemer vangt niet aan met uitvoering van de test zonder schriftelijke goedkeuring door Deelnemer van genoemde documenten dan wel een afwijking hierop.	X	X
B3.8	In de Aanvraag kan Deelnemer eisen dat een door betrokken partijen getekende *NOK bijlage xx - Verwerkersovereenkomst* een noodzakelijke voorwaarde is voor het starten van de opdracht (. Dat zal geëist worden als Opdrachtnemer bij de uitvoering van de opdracht toegang kan krijgen tot persoonsgegevens. Opdrachtnemer vangt dan niet aan met uitvoering van de test zonder een door betrokken partijen getekende Verwerkersovereenkomst.	X	X
B3.9	Bij aanvang van de Opdracht dienen alle medewerkers die deelnemen aan de Opdracht aantoonbaar in het bezit zijn van een geldige VOG (screeningsprofiel 11, 12 en 41) en VGB indien vereist in de Aanvraag.	X	X
B3.10	Opdrachtnemer legt in beginsel aan de op te leveren rapportages en onderliggende documenten geen belemmeringen aan Deelnemer op met betrekking tot het beschikbaar stellen, verspreiden, opslaan en distribueren. Bijvoorbeeld aan rechthebbende derde partijen die eigenaar of beheerder zijn van onderzochte/geteste objecten of door Deelnemer ingeschakelde auditors. Deelnemer draagt in zo'n geval de verantwoordelijkheid voor het verder verspreiden van deze informatie en de vertrouwelijkheid hiervan. Eventuele door Deelnemer en Opdrachtnemer gemaakte afspraken over vertrouwelijkheid worden in de rapportage benoemd en gerespecteerd. Opdrachtnemer accepteert dat Deelnemer de intellectuele eigendomsrechten heeft op de data die afkomstig is van Deelnemer en door opdrachtnemer opgestelde rapportages. Opdrachtnemer deelt de rapportage niet zonder expliciete toestemming van de contactpersoon van Deelnemer met anderen.		
Voorbereidingsfase *Dit gedeelte omvat eisen die betrekking hebben ter voorbereiding van het uitvoeren van Red Teaming testen en hebben veelal betrekking op scope en planning aspecten.*		**ART**	**TIBER**
B3.11	Deelnemer verschaft voor aanvang werkzaamheden (na gunning) aan Opdrachtnemer een scoping document conform *NOK bijlage xx –*	X	X

	Scoping document. Dit beschrijft de daadwerkelijke scope van de RT test (organisatie, processen, techniek), de kritieke functies van de organisatie en de systemen, processen en mensen die deze faciliteren. Daarnaast worden voor de systemen de beoogde vlaggen benoemd. Een Vlag is een aantasting van de beschikbaarheid, vertrouwelijkheid en of integriteit. (Bijvoorbeeld het kunnen uitvoeren van ransomware op een systeem is een aantasting van de beschikbaarheid)		
B3.12	De Opdrachtnemer oriënteert zich op het dreigingslandschap specifiek voor de Deelnemer	X	X
B3.13	De Opdrachtnemer neemt deel aan de Launch-meeting. Hierbij worden o.a. het concept plan van aanpak, en eventueel benodigde leg-ups besproken.	X	X
B3.14	De Opdrachtnemer neemt deel aan de Business Overview workshop waarbij het Control team inzicht geeft in de organisatie, kaders stelt en andere aanvullingen geeft op het concept plan van aanpak.	X	X
B3.15	De Opdrachtnemer scherpt het plan van aanpak aan o.b.v. input van de deelnemers in de Launch-meeting en Business Overview workshop. Onderdeel van dit plan zijn ook de rules of engagement, die ten minste het volgende bevatten: - Een algemene beschrijving van de technieken die worden gebruikt tijdens de aanval; - Een lijst met uitgesloten technieken - Een gedetailleerde beschrijving van scenario's die worden gebruikt voor social engineering; - Hoe de privacy van zowel vrijwillige als onvrijwillige deelnemers wordt gewaarborgd in overeenstemming met de regels en voorschriften.	X	X
B3.16	Opdrachtnemer presenteert en verduidelijkt aannames en risico's in het plan van aanpak (onderdeel van de offerte). Deelnemer besluit of Opdrachtnemer kan doorgaan naar de testfase of dat het plan van aanpak verder aangepast dient te worden. Het plan van aanpak kan echter niet meer wezenlijk gewijzigd worden.	X	X
Testfase *Dit gedeelte omvat eisen die betrekking hebben op testfase van een ART-rijk of TIBER rijk test*		**ART**	**TIBER**
B3.17	Deelnemer verschaft Opdrachtnemer een Targeted Threat Intelligence (TTI/TI) rapport, als Deelnemer heeft besloten om TI-rapport door een derde (onafhankelijke Threat Intelligence (TI) Provider) te laten opstellen. Dit rapport bevat o.a.: o Een beknopt organisatie specifiek dreigingsbeeld (welke actoren zijn geïnteresseerd in de Deelnemer, wat is hun motivatie en achtergrond). o Relevante open source intelligence (welke informatie is er online over de doelwit organisatie te vinden die gebruikt kan worden in de aanval). o Bij elke opdracht zal het (minimaal) aantal threat intelligence gebaseerde scenario's door de Deelnemer bepaald worden.	X	X

	○ Deelnemer geeft aan welke scenario's in de Red Teaming fase doorlopen dienen te worden. Deelnemer kan besluiten het TI-rapport door Opdrachtnemer te laten opstellen, maar dan dient het TI-rapport volledig onafhankelijk, met andere deskundigen dan in de Red teaming testfase en onder strikte geheimhouding tot stand te komen. De Deelnemer kan nadere voorwaarden stellen aan de onafhankelijkheid en vertrouwelijkheid van deze TI-fase en toetsen op te nemen en genomen maatregelen hieromtrent.		
B3.18	Door Deelnemer wordt een overdrachtssessie georganiseerd met TI-provider en Opdrachtnemer, waarin een gedetailleerde uitleg wordt gegeven over het Targeted Threat Intelligence (TTI)-rapport en mogelijke dreigingsscenario's voor de test worden besproken. Opdrachtnemer dient inzicht te verkrijgen uit deze overdrachtssessie en het document met de scopespecificatie en het TTI-rapport verder te bestuderen om het Red Team-testplan op te stellen. Deze informatie en documentatie vormen de bewijsbasis voor het ontwerpen en rechtvaardigen van het voorgestelde Red Team-testplan en de aanvalsscenario's.	X	X
B3.19	Bij een TIBER-rijk test worden door Opdrachtnemer twee volledige scenario's en een *scenario X* uitgewerkt en uitgevoerd. Het doel van scenario X is om vooruit te kijken naar welke geavanceerde aanvallen in de (nabije) toekomst te verwachten zijn. Dit scenario kan gericht zijn op een bepaalde innovatieve techniek, op tactieken die de Opdrachtnemer en TIP zien ontwikkelen, mogelijk in combinatie met maatschappelijke ontwikkelingen of ontwikkelingen in het dreigingslandschap die in de toekomst van invloed zullen zijn op de entiteit.		X
B3.20	Bij een ART-rijk test worden het aantal en type scenario's dat dient te worden uitgewerkt en uitgevoerd door Deelnemer nader gespecificeerd in de Offerteaanvraag.	X	
B3.21	De Opdrachtnemer levert een RT-testplan op met daarin: ○ Een beschrijving van de aanvals-scenario's conform ART of TIBER (zie hierboven) op basis van de threat intelligence. ○ Een beschrijving van de kwaadwillende actor(en), zijn/hun motivatie en achtergrond gebaseerd op het TI rapport. ○ Waar nodig een aanvullend overzicht van de OSINT ter aanvulling op het TI-rapport. ○ Een beschrijving van de Rules of Engagement met o.a. de in te zetten techniek, tactieken en privacy waarborging. ○ De planning van de cyberaanval in activiteiten en tijd. ○ Informatie over de testfase, met o.a. aangewezen specialisten, eventueel benodigde leg ups en mogelijke risico's. *Een Leg up is een hulpmiddel om een stap verder te komen of (tijdelijk) over te slaan in de kill chain van de aanval. Voorbeelden zijn: een account + wachtwoord, toegang tot een gebouw of inzicht in het netwerk.* ○ Het projectteam van Opdrachtnemer en het control team identificeren bijkomende risico's, zoals C2000 criteria en stellen een mitigatieplan op. C2000 criteria worden gehanteerd om risico's ten aanzien van spionage, beïnvloeding of sabotage door		

	statelijke actoren of andere derde partijen te beoordelen. Zie Kamerstukken II 2018/19, 25 124, nr. 96. Algemene Inlichtingen- en Veiligheidsdienst, (2019), Offensief cyberprogramma een ideaal businessmodel voor Staten. o Een beschrijving van de afrondingsfase. o Een saneringsplan. (Het opruimen na de test, verwijderen van gebruikte malware, etc.)		
B3.22	De Opdrachtnemer presenteert het RT-testplan aan de Deelnemer voor akkoord. Pas na akkoord van Deelnemer kan de testuitvoering starten. Indien nodig wordt het RT-testplan aangepast tot er voldoende draagvlak is voor een go.	X	X
B3.23	De Opdrachtnemer voert de test uit zoals beschreven in het RT-testplan en de eerder gekozen scenario's worden uitgevoerd volgens de juiste TTP's / modus operandi, passend bij de actor(en)	X	X
B3.24	Indien in de testfase om welke reden dan ook moet worden besloten het testen 'onder de radar' te beëindigen (bijvoorbeeld omdat de test gedetecteerd is) zullen de resterende testactiviteiten (scenario's) na overleg met Deelnemer (Control Team en TCT-rijk) alsnog worden uitgevoerd in een passende werkvorm, bijvoorbeeld purple teaming. (NB: dit is niet de purple teaming sessie die in de leerfase wordt gevraagd)	X	X
B3.25	Gedurende de voorbereidings- en testfase vindt er minimaal wekelijks een meeting plaats tussen Opdrachtnemer en Deelnemer (Control Team en TCT-rijk).	X	X
B3.26	Tijdens de testfase is er nauw contact tussen RT-provider en Deelnemer (Control Team en TCT-rijk). Risicovolle activiteiten mogen pas uitgevoerd worden na expliciet akkoord door CT-lead. (nb: in de praktijk wordt hier vaak een signalgroep o.i.d. voor gebruikt)	X	X
Afrondings- & leerfase *Dit gedeelte omvat eisen betreffende afrondings- en leerfase en hebben veelal betrekking op rapportage- en kennisdeling aspecten.*		**ART**	**TIBER**
B3.27	De Opdrachtnemer levert binnen 30 dagen na afronding van de RT-test een concept RT-testrapport op in het RT-test report format, waarin de toegepaste technieken, de duur van de aanval, een tijdlijn en een gedetailleerde beschrijving van de resultaten van de aanval worden beschreven. Het rapport geeft een overzicht van het hele RT-proces. Daarbij horen de kritieke systemen, de gebruikte Threat Intelligence, vooronderzoek, de geplande en uitgevoerde scenario's, de testbevindingen en het beveiligingsadvies aan de organisatie.	X	X
B3.28	Daarnaast levert de Opdrachtnemer ook een samenvatting (Test summary) op voor de bestuurlijke top van de organisatie van de Deelnemer, op basis van het RT-testrapport.	X	X
B3.29	Zowel het RT-testrapport als de samenvatting dienen in het Nederlands te worden opgeleverd.	X	X
B3.30	De Opdrachtnemer faciliteert een replay-sessie voor het Blue team van Deelnemer. Hierbij geeft het RT van Opdrachtnemer inzicht aan het Blue Team welk soort aanvallen er zijn uitgevoerd. (NB: deze	X	X

	replay sessie kan op verzoek van deelnemer worden gecombineerd met de Purple Teaming sessie.		
B3.31	De Opdrachtnemer faciliteert de Purple Teaming sessie met Deelnemer (het Blue Team, het Control Team en TCT-rijk). Opdrachtnemer faciliteert hierbij een workshop van ten minste twee volle dagen waarbij de aanvalspaden stap voor stap worden doorgenomen met de beveiligingsorganisatie en de dialoog over de aanvallen plaatsvindt. Het TCT-rijk heeft hierbij een adviserende rol. Deelnemer kan besluiten dat volstaan wordt met een kortere workshop.	X	X
B3.32	Na de Purple teaming sessie wordt het definitieve testrapport door Opdrachtnemer opgeleverd met aanvullingen vanuit de Purple teaming sessie.	X	X
B3.33	In deze fase wordt er ook een 360-graden-feedback meeting georganiseerd door het TCT-rijk om het ART- of TIBER-rijk proces te evalueren. De Opdrachtnemer is hierbij aanwezig en participeert actief. Tijdens deze bijeenkomst komen de Deelnemer, TCT, TI-Provider en Opdrachtnemer samen om de test te evalueren. Het doel is om de leerervaring van iedereen die betrokken is bij het proces voor toekomstige RT-testen verder te faciliteren.	X	X
B3.34	De Opdrachtnemer is drie (3) maal een (1) uur beschikbaar in de afrondings- en leerfase voor medewerkers die uitvoering moeten geven aan de bevindingen en aanbevelingen die uit deze opdracht naar voren zijn gekomen. Indien nodig in persoon. Dit staat los van de sessies die worden gehouden tijdens de Purple teaming fase.	X	X
B3.35	De Opdrachtnemer is op verzoek van Deelnemer beschikbaar om Deelnemer te faciliteren in het organiseren van een Gold Teaming. Het exact aantal uren zal door Deelnemer in Offerteaanvraag worden benoemd. Nb: de Gold Teaming wordt door andere leverancier verzorgd, het gaat hier puur ter ondersteuning/toelichting op het scenario.	X	
B3.36	Na afronding (en acceptatie door Deelnemer) van alle activiteiten voor de opdracht dient Opdrachtnemer alle informatie die hij gedurende de uitvoering van de opdracht heeft verzameld te vernietigen. De vernietiging van de informatie dient, binnen 30 kalenderdagen na acceptatie van geleverde diensten, vanuit het management van de Opdrachtnemer formeel bekrachtigd te worden. Voor het vernietigen van de informatie dient te worden voldaan VIR, VIR-BI en BIO.	X	X