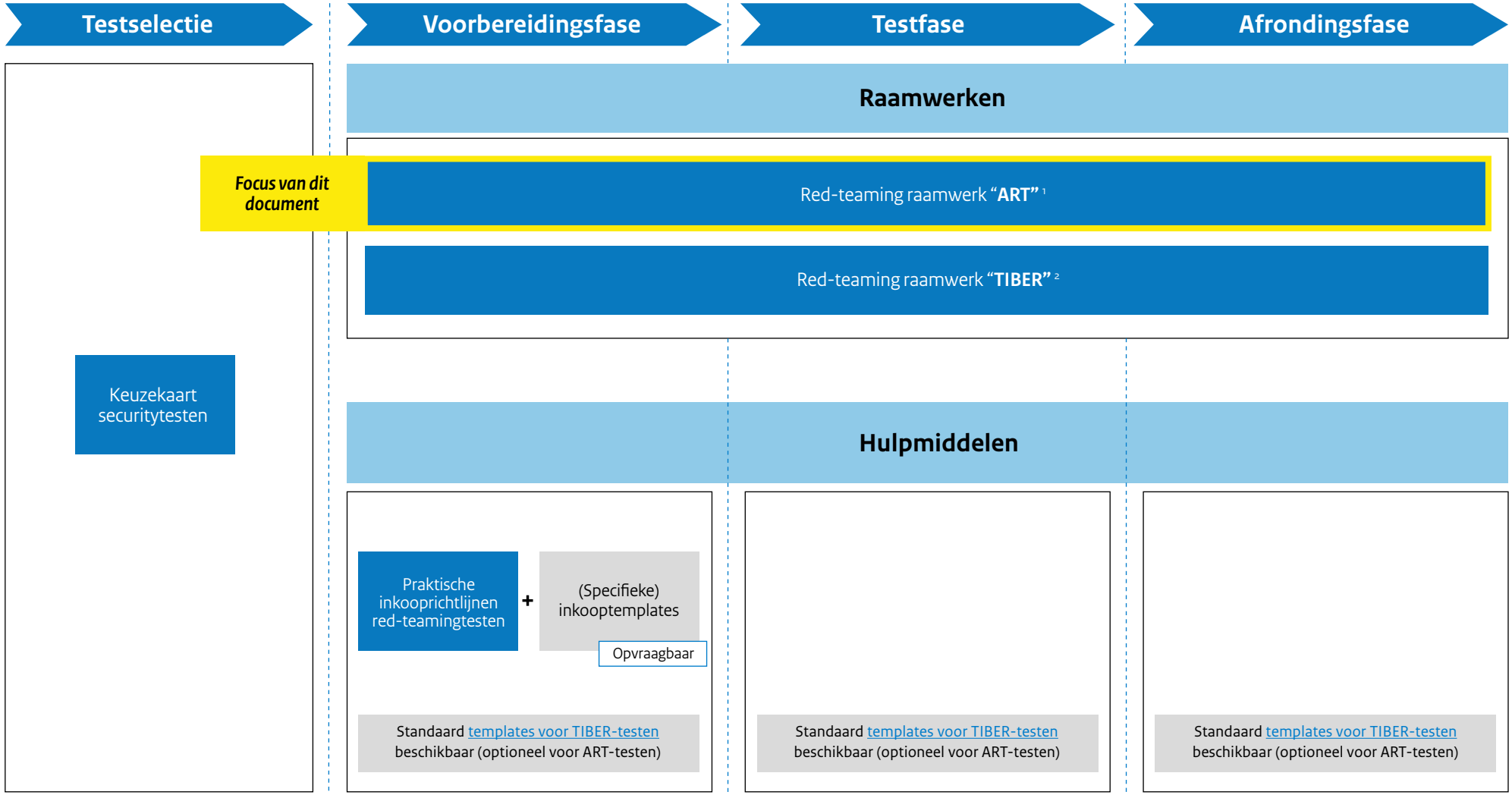
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

# Red-teaming raamwerk “Advanced Red Teaming (ART)”

Versie: 1.0
Datum: maart 2023

Directie CIO Rijk

# Basis gereedschapskist red-teamingtesten




[1] ART: *Advanced Red Teaming*

[2] TIBER: *Threat Intelligence Based Ethical Red-teaming*

# Introductie op Advanced Red Teaming (ART)

### Wat is ART?

De Nederlandsche Bank (DNB) ontwikkelt samen met de Rijksoverheid het Advanced Red Teaming (ART)-raamwerk. Dit raamwerk wordt ontwikkeld als lichtere variant voor het TIBER-raamwerk. Het ART-raamwerk is enerzijds bedoeld voor het testen van de beveiliging van Te Beschermen Belangen (kroonjuwelen) met een midden – zeer hoog classificatieniveau en anderzijds bedoeld als opmaat naar een TIBER-test (voor organisaties waar de drempel voor het uitvoeren van een uitgebreidere TIBER test nog te hoog is). Voor een introductie op TIBER, zie het red-teaming raamwerk 'TIBER'.

### Wat is het verschil ten opzichte van een TIBER-test?

Het verschil met TIBER is dat er maar één dienstverlener (een red-team provider) wordt gecontracteerd. Deze voert op basis van (sector)generieke threat intelligence en een verkenningsfase slechts één aanvalsscenario uit. Hiermee worden de kosten t.o.v. een TIBER-test aanzienlijk verlaagd en wordt de doorlooptijd korter. De betrokkenheid van het TCT (TIBER Cyber Team) Rijk[3] is meer georganiseerd rondom vaste momenten in de test in plaats van op continue basis. Andere eisen vanuit het TIBER-raamwerk blijven van kracht. Zie pagina 4+5 voor een nadere uitwerking.

*N.b. De TIBER-templates zijn optioneel voor een ART-test, maar kunnen een goed startpunt zijn voor documentatie.*

### Is mijn organisatie toe aan een ART-test?

Of uw organisatie toe is aan ART-testen hangt samen met het volwassenheidsniveau van de organisatie. De volwassenheid komt in de basis neer op de inrichting van de security organisatie gecombineerd met de implementatiestatus van de verschillende security-testen. Voor meer informatie over welke type securitytest past bij uw organisatie en testdoel, ga naar het hulpmiddel 'Keuzekaart securitytesten' (onderdeel van de gereedschapskist).

### Over dit document

Het ART-raamwerk is nog in ontwikkeling en wordt door de DNB in samenwerking met de Rijksoverheid uitgewerkt op basis van pilots. Dit document is een eerste uitwerking van ART en betreft een vergelijking ten opzichte van het uitgebreidere TIBER-raamwerk (TIBER-NL guide van DNB). Hierin wordt aangegeven welke zaken vanuit het TIBER-raamwerk verplicht en optioneel zijn voor een ART-test. Samen met de DNB wordt toegewerkt naar een handreiking specifiek voor ART. Wanneer deze gereed is, wordt deze toegevoegd aan de gereedschapskist.

### Contactpersoon

Voor vragen over of terugkoppeling op documenten uit de gereedschapskist, neem contact op met de Red-teaming coördinator via het mailadres redteaming@rijksoverheid.nl.

[3] Het TCT (TIBER Cyber Team) voor de Rijksoverheid is nog in ontwikkeling.

# Kenmerken Advanced Red Teaming (ART) t.o.v. TIBER

Het ART-raamwerk is (vooralsnog) uitgewerkt als een vergelijking t.o.v. de TIBER-NL guide. Onderstaande tabel geeft inzicht in de belangrijkste vereisten van een TIBER-test. In de kolom “toepassing ART” zijn in het licht blauw zaken uitgelicht die voor een ART-test afwijkend zijn ten opzichte van een TIBER-test. De DNB ontwikkelt in samenwerking met de Rijksoverheid een handreiking voor een ART-test waarin praktijkervaring vanuit pilots wordt verwerkt.

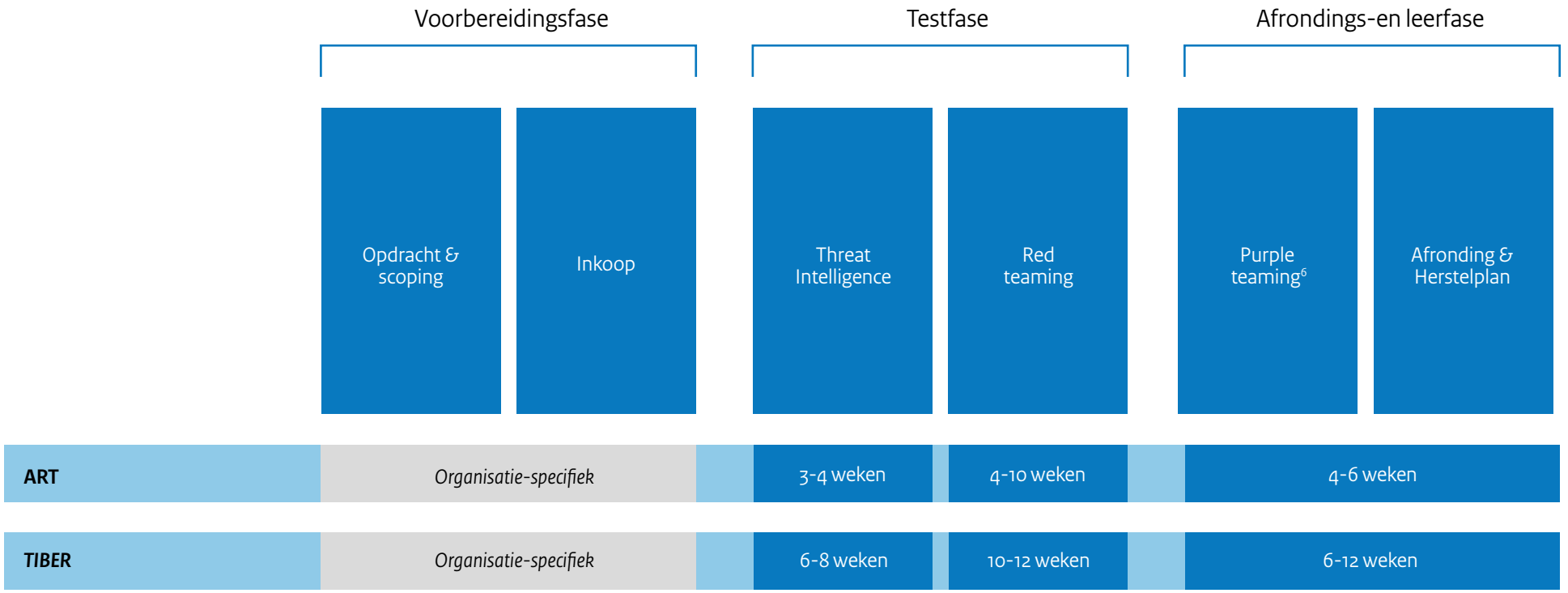
| Nr | Belangrijkste TIBER vereisten | Toepassing ART | Opmerkingen t.a.v. ART |
|---|---|---|---|
| 1 | Gericht op **kritieke functies** van de organisatie inclusief mensen, processen en technologie. | Ja | *TIBER vereiste is van toepassing voor een ART-test.* |
| 2 | Een **generiek dreigingsbeeld (GTL)** voor de sector wordt ontwikkeld (door het TCT). | Optioneel | Het generieke dreigingsbeeld (GTL) is geen vereiste voor een ART-test. |
| 3 | Documenteren van **scope** in TIBER Scope Specification template geaccordeerd een bestuurder uit de executive board. | Ja | Het gebruik van het TIBER - Scope Specification Template is optioneel. |
| 4 | Het **TIBER Cyber Team (TCT)**[4] draagt er zorg voor dat een test wordt uitgevoerd op een uniforme en gecontroleerde manier. | Deels | Het TCT is inhoudelijk betrokken bij vaste momenten: Bij de pre-launch (voorafgaand aan inkoop), bij het vaststellen van de scope en het vaststellen van het testplan (aanvalsscenario). Een wekelijks afstemmoment is optioneel. |
| 5 | **Threat Intelligence** (TI) wordt uitgevoerd door een onafhankelijke TI dienstverlener. | Optioneel | Er wordt een TI gebaseerde verkenningsfase uitgevoerd waarin generieke dreigings-beelden specifiek worden gemaakt voor de te testen organisatie.<br>Inzet van een TI-dienstverlener is optioneel. |
| 6 | **Red teaming** (RT) wordt uitgevoerd door een onafhankelijke RT dienstverlener. | Ja | *TIBER vereiste is van toepassing voor een ART-test.* |
| 7 | De red-teamingtest wordt uitgevoerd op **live productiesystemen.** | Ja (tenzij) | Principe ‘pas toe of leg uit’ wordt gehanteerd. De ART test kan worden opgeknipt als een bepaald deel van het testtraject teveel risico oplevert (bijv. bij OT-systemen). |
| 8 | Het betreft een **end-to-end test** (van buiten naar binnen). | Optioneel[5] | De (te testen) organisatie bepaalt zelf of het een end-to-end test is of dat wordt uitgegaan van een ‘assume breach’ scenario. |
| 9 | Het ontwikkelen van **meerdere aanvalsscenario’s** (≥ 2) gebaseerd op onafhankelijke dreigingsinformatie. | ≥ 1 | Minimaal 1 aanvalsscenario is vereist voor een ART-test. |
| 10 | Het opleveren van een **Targeted Threat Intelligence (TTI) Report.** | Optioneel | Er wordt een TI gebaseerde verkenningsfase uitgevoerd waarin generieke dreigings-beelden specifiek worden gemaakt voor de te testen organisatie.<br>Het gebruik van het TIBER - TTI Report is optioneel. |
| 11 | Het opstellen van een **Red team Test Plan.** | Ja | Het gebruik van het TIBER - Red Team Test Plan is optioneel. |
| 12 | Het opleveren van een **Red team test report** en Blue team report. | Ja | Het gebruik van het TIBER – Red Team Test Report is optioneel. |
| 13 | Een **Purple teaming oefening** wordt uitgevoerd om de leerervaring van de geteste organisatie te vergroten. | Ja | *TIBER vereiste is van toepassing voor een ART-test.* |
| 14 | **Een Test summary report** wordt gebruikt voor kennisdeling (o.a. binnen de WTL community). | Ja | Het gebruik van het TIBER – Test Summary format is optioneel. N.b. voor ART werken we toe naar 1 rapport voor de gehele afrondings- en leerfase. |
| 15 | Een **verklaring** wordt afgegeven door het TCT, de entiteit en de TI/RT dienstverlener(s) dat de test is uitgevoerd cf. vereisten. | Ja | N.b. voor ART werken we toe naar één rapport voor de gehele afrondings- en leerfase. De verklaring van alle betrokken partijen wordt hierin meegenomen. |

[4] Het TCT (TIBER Cyber Team) voor de Rijksoverheid is nog in ontwikkeling.

[5] Afhankelijk van privacy vraagstuk: Voor de Rijksoverheid hanteren we voor een TIBER test een assume breach scenario totdat het aandachtspunt rondom omgang met persoonsgegevens is uitgezocht.

# Doorlooptijd ART-test (t.o.v. TIBER-test)

**Doorlooptijden**
Een ART-test is een lichtere variant van een TIBER-test en kent een kortere doorlooptijd in vergelijking met een TIBER test. Het onderstaande overzicht geeft een indicatie van doorlooptijden per fase van een ART-test ten opzichte van een TIBER-test.




[6] Let op: Binnen het TIBER raamwerk is purple teaming een fase van een TIBER-test (zie bovenstaande afbeelding). Purple teaming kan ook als een separate securitytest worden ingezet.

Dit is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties
Postbus 20011 | 2500 EA Den Haag

maart 2023