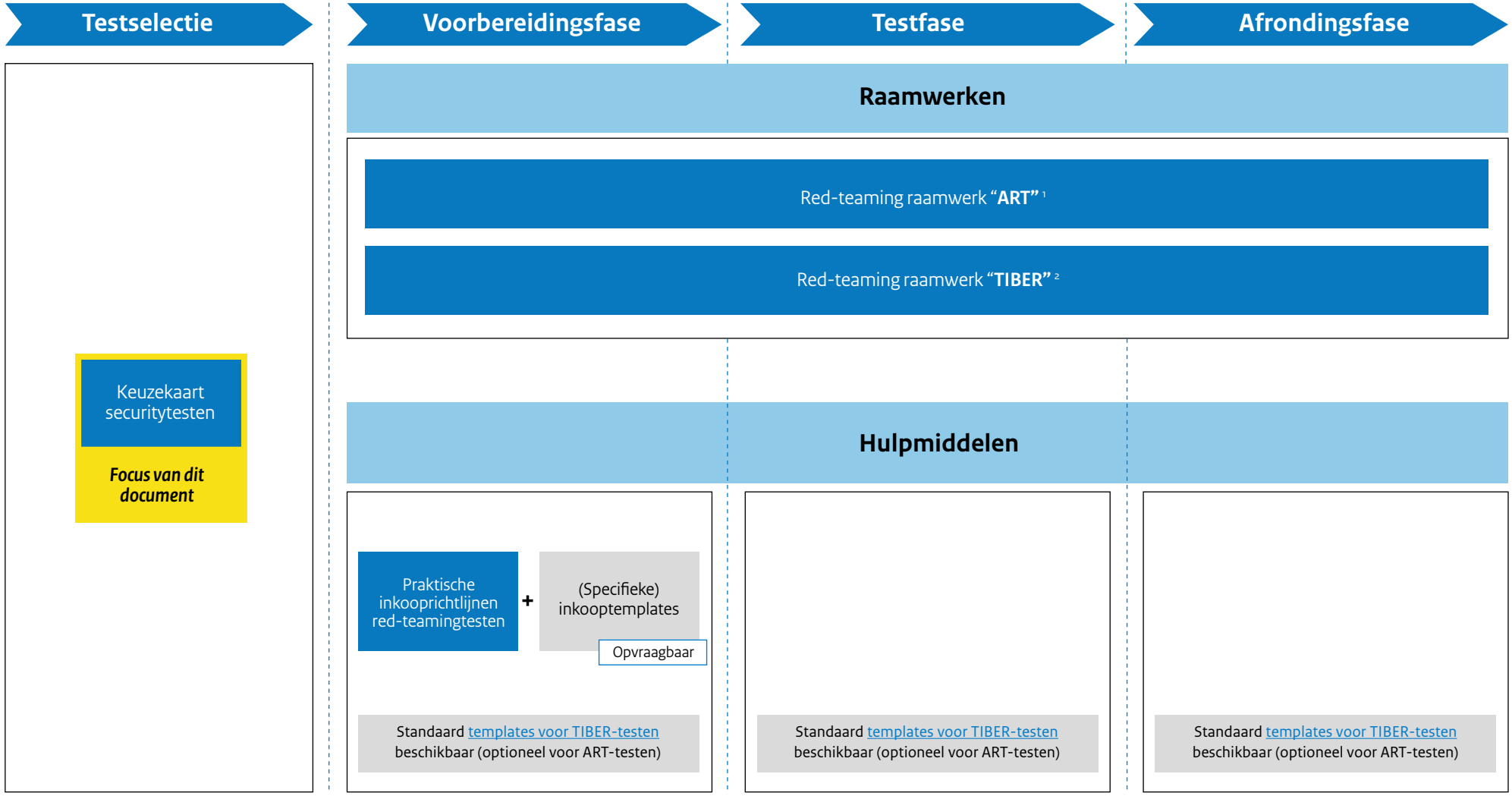
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Keuzekaart securitytesten

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*

Keuzekaart securitytesten - introductie en toelichting

Doel

Securitytesten[3] hebben als doel om de werking van weerbaarheidsversterkende maatregelen te toetsen.

De keuzekaart helpt bij het beantwoorden van de vraag: Welk type securitytest is geschikt voor mijn testdoel?

N.B. de keuzekaart gaat over het inzetten van securitytesten op departementale of hogere Te Beschermen Belangen (TBB). Dit is aanvullend op het reguliere testen van nieuwe en gewijzigde IT (en OT) omgevingen, wat wordt beschouwd als het basisniveau.

Type testen

De volgende type securitytesten zijn opgenomen in de keuzekaart:

- Vulnerability scan
- Pentest
- Purple teaming
- Red teaming - ART
- Red teaming - TIBER

Adviezen voor gebruik

- Zorg dat het testdoel en de scope van de te testen omgeving helder is.
- Zorg voor een lijnverantwoordelijke van de test (eigenaar/verantwoordelijke voor de te testen omgeving). Deze persoon beslist over welk type test wordt uitgevoerd.
- Advies is om te redeneren vanuit de TBB-classificatie bij het selecteren van een securitytest.
- Maak met de lijnverantwoordelijke afspraken over de omvang van het budget* – dit is van invloed op de keuze voor een type test.
- Is er een IT-leverancier betrokken bij de te testen omgeving? Betrek deze dan bij het maken van de keuze voor een type test.
- Bespreek eventuele dilemma's met de CISO.
- Bij vragen over de keuzekaart securitytesten, neem contact op met de Red-teaming coördinator (redteaming@rijksoverheid.nl).

** Tip: Houd vooraf ook rekening met capaciteit en middelen voor het oplossen van de bevindingen.*

Elementen van de keuzekaart

Type test	Binnen de testtypen zijn nog diverse keuzes mogelijk, af te stemmen met de testende partij.
Kenmerk	Van boven naar beneden is globaal een toename in complexiteit en "heimelijkheid".
Doel / aanpak	Wat wil je bereiken met de test (vanuit het perspectief van de tester)? Kies primair daar een geschikt type test bij.
Scope dimensies	Dit is direct gerelateerd aan het type test; de keuze om naast techniek ook de processen en menselijk gedrag onderdeel te maken van de test.
NIST functies	Het Cybersecurity Framework | NIST kent vijf basis functies: identify, protect, detect, respond, recover. Aangegeven is op welke functies het type test betrekking heeft.
Minimale volwassenheid	Geeft een indicatie voor de geadviseerde minimale volwassenheid voor het beste rendement van de test. Dit is afgeleid van het Volwassenheidsmodel informatiebeveiliging (nba.nl). Het kent 5 niveaus van volwassenheid 1-5: initieel, herhaalbaar, gedefinieerd, beheerst & meetbaar en continu verbeteren.
TBB-classificatie primair doel	Geeft aan voor welk type Te Beschermen Belang (TBB)[4]de test het meest geschikt is, gezien de investering. TBB classificatie is gebaseerd op de Leidraad Te Beschermen Belangen
Indicatie tijdsbesteding testfase	Tijdsbesteding voor het uitvoeren van de test. De benodigde tijd geeft een grove indicatie van de investering (€). (Hierop is de tabel gesorteerd).
Aanbevolen ervaring	Geeft aan wat de benodigde ervaring is voor het beste rendement van de test.
Hulpmiddelen	Geeft een verwijzing naar hulpmiddelen voor het uitvoeren van de test.

[3] Securitytesten is het evalueren van de beveiligingsmaatregelen van een systeem zoals deze zijn toegepast binnen een operationele omgeving om de weerbaarheid van dat systeem te bepalen [NCSC-TG-004]. Het wordt gekenmerkt door een proces waarbij één of meer testobjecten aan gespecificeerde omstandigheden worden onderworpen om werkelijk met verwacht gedrag te vergelijken [NIST SP 800-53A Rev. 5].

[4] Te Beschermen Belangen: Informatie, systemen, materieel, goederen, (bewinds)personen en objecten die beveiligd moeten worden om de werking van de Rijksoverheid zoveel mogelijk doorgang te laten vinden. Kennisname of aantasting hiervan door vreemde mogendheden of derden kan de Nationale Veiligheid, het algemeen (economisch/politiek) belang en/of de integriteit van de Rijksoverheid aantasten.

Keuzekaart securitytesten

Vragen?
stuur een mail naar
redteaming@rijksoverheid.nl

Welk type securitytest is geschikt voor mijn testdoel?

	Type test	Kenmerk	Doel / aanpak	Scope dimensies	NIST-functies (NIST cybe-security framework)	Minimale volwassenheid (NBA model niveau 1-5)	TBB-classificatie primair doel	Indicatie tijds-besteding testfase	Aanbevolen ervaring	Hulpmiddelen
Basisniveau	**Vulnerability scan (VS)**	Geautomatiseerde scans op technische kwetsbaarheden	In de breedte van de techniek opsporen van bekende technische kwetsbaarheden	Techniek	Identify, protect	Niveau 1 “initieel” of hoger	Alle classificaties	1-2 dagen	• Geen	handreiking kwetsbaarheidsscan
	Pentest	Cyber aanval “boven de radar” uitgevoerd met tools en handmatige acties	Gericht op 1 of beperkt aantal systemen. Kwetsbaarheden opsporen en deze gebruiken om binnen te komen	Techniek	Identify, protect, detect	Niveau 1 “initieel” of hoger	Alle classificaties	1-2 weken	• VS uitgevoerd en bevindingen (grotendeels) opgevolgd	Whitepaper pentesten
Geavanceerde securitytesten	**Purple teaming**[5]	Cyberaanval uitgevoerd door het red team in samenwerking met het blue team	Verbeteren van de effectiviteit van het blue team om daarmee de cyber weerbaarheid te verhogen	Techniek, mensen, processen	Identify, protect, detect, respond	Niveau 2 “herhaalbaar” of hoger	Midden tot (zeer) hoog	2-10 weken	• VS en evt. pentest uitgevoerd en bevindingen (grotendeels) opgevolgd • Monitoring en detectie-capaciteit ingericht en operationeel	Purple teaming guide (TIBER)
	Red teaming – ART[6]	Cyberaanval “onder de radar” gebaseerd op generieke dreigingsinformatie	Simuleren van een specifieke actor[7] om te kijken in hoeverre de kroonjuwelen/Te Beschermen Belangen (TBB) hiertegen beschermd zijn en de organisatie als geheel hiervan te laten leren	Techniek, mensen, processen	Identify, protect, detect, respond	Niveau 2 “herhaalbaar” of hoger	Midden tot (zeer) hoog	7–14 weken	• VS en pentest uitgevoerd en bevindingen (grotendeels) opgevolgd • Monitoring en detectie-capaciteit ingericht en operationeel	Zie RT-raamwerk ART (in de gereedschapskist)
	Red teaming – TIBER[8]	Cyberaanval “onder de radar” gebaseerd op onafhankelijke org. specifieke dreigingsinformatie		Techniek, mensen, processen	Identify, protect, detect, respond	Niveau 3 “gedefinieerd” of hoger	(Zeer) hoog	16–20 weken	• VS en pentest uitgevoerd en bevindingen (grotendeels) opgevolgd • SOC[9] ingericht en operationeel • Ervaring met red-/purple-teamingtesten	Zie RT-raamwerk TIBER (in de gereedschapskist)

[5] Purple teaming: dit kan zowel een separate securitytest zijn als een fase binnen een red-teamingtest. N.b. de purple teaming guide is gericht op purple teaming als fase binnen een red-teamingtest. Nog geen guide beschikbaar voor een separate purple-teamingtest
[6] ART: Advanced Red Teaming
[7] Dreigingsactor: een individu of een groep die een dreiging vormt, bijv. statelijke actoren of criminele groeperingen
[8] TIBER: Threat Intelligence Based Ethical Red-teaming
[9] SOC: Security Operations Center

Dit is een uitgave van:

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

maart 2023