mbo digitaal

Weerbaarheidstesten in het mbo

Traject ‘van check tot hack’

Joost Gadellaa & Mick Deben

25 juni 2025

1.0

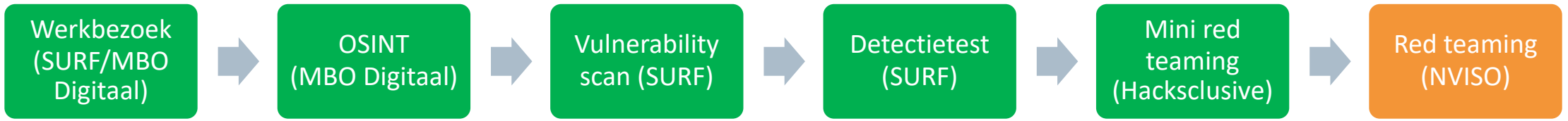
mbo digitaal

mbo digitaal

mbo digitaal

Traject van check tot hack

- Tien deelnemende MBO's
- Drie gaan door tot een 'echte' red teaming
- *In verschillende stappen geleidelijk verbeterpunten identificeren, zodat offensieve tests zo effectief mogelijk benut worden*
  - Wegnemen van laaghangend fruit, niet met een kanon op een mug schieten
  - Punten identificeren waar MBO Digitaal/SURF kan helpen met technische weerbaarheid
- Geleerde lessen in onze trendrapportage (SCIPR/RT)



mbo digitaal

Greep uit de ervaringen van deelnemende instellingen

- “Het traject heeft ons geholpen om MFA voor studenten (eindelijk) af te mogen dwingen”
- “De samenwerking in onze keten (belangrijkste IT-leverancier) is door dit traject versterkt”
- “Bij ons onbekende bevindingen, zoals gelekte credentials en public-facing kwetsbaarheden, waren enorm waardevol”

mbo digitaal

Ervaringen van Aventus (Hendri Boer)

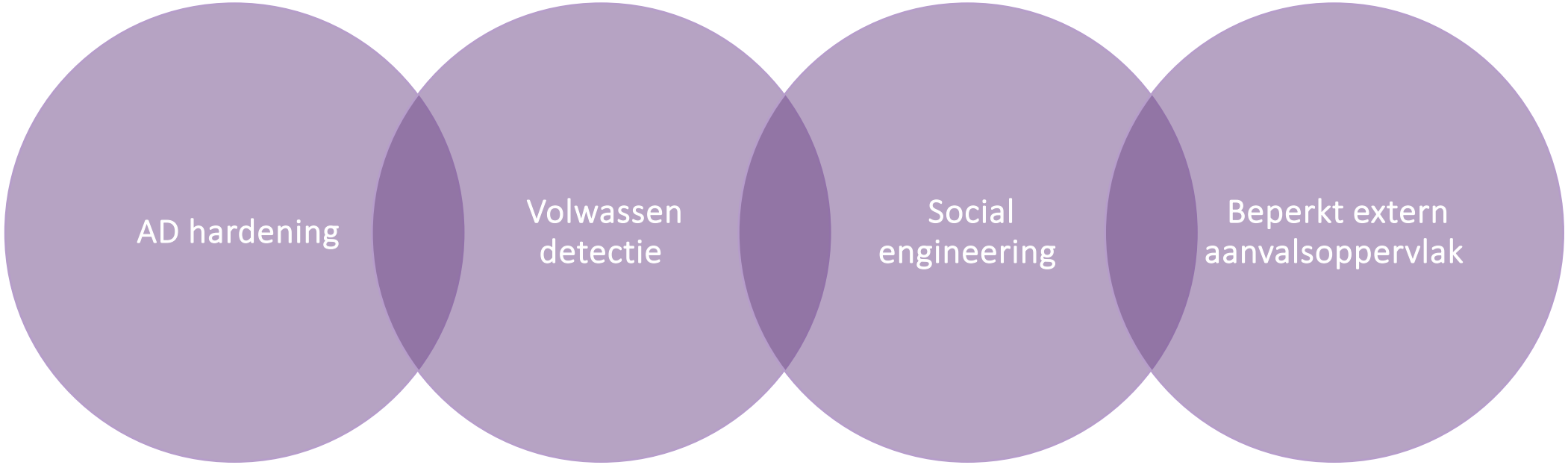
1. Hoe heeft het traject waarde toegevoegd voor Aventus?

2. Hoe heb je de red teaming ervaren?

3. Wat was het hoogtepunt voor Aventus?

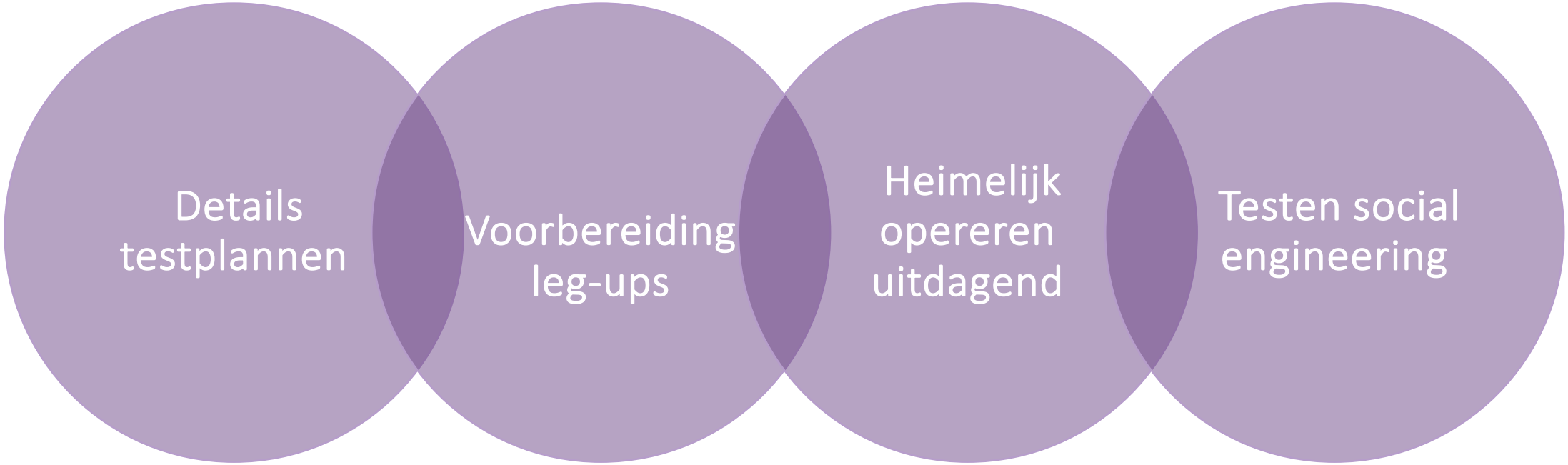
mbo digitaal

Red teaming geleerde lessen (bevindingen)



mbo digitaal

Red teaming geleerde lessen (proces)



mbo digitaal

Handreikingen

- Weerstand bieden tegen MitM aanvallen
- Weerstand bieden tegen ransomware
- Handreiking TLS
- Handreiking beveiligen e-mail
- Handreiking cybersecurity configuraties in netwerken
- Handreiking identificeren infecties
- Identificeren en oplossen van misconfiguraties en kwetsbaarheden in AD/Entra ID en M365

mbo digitaal

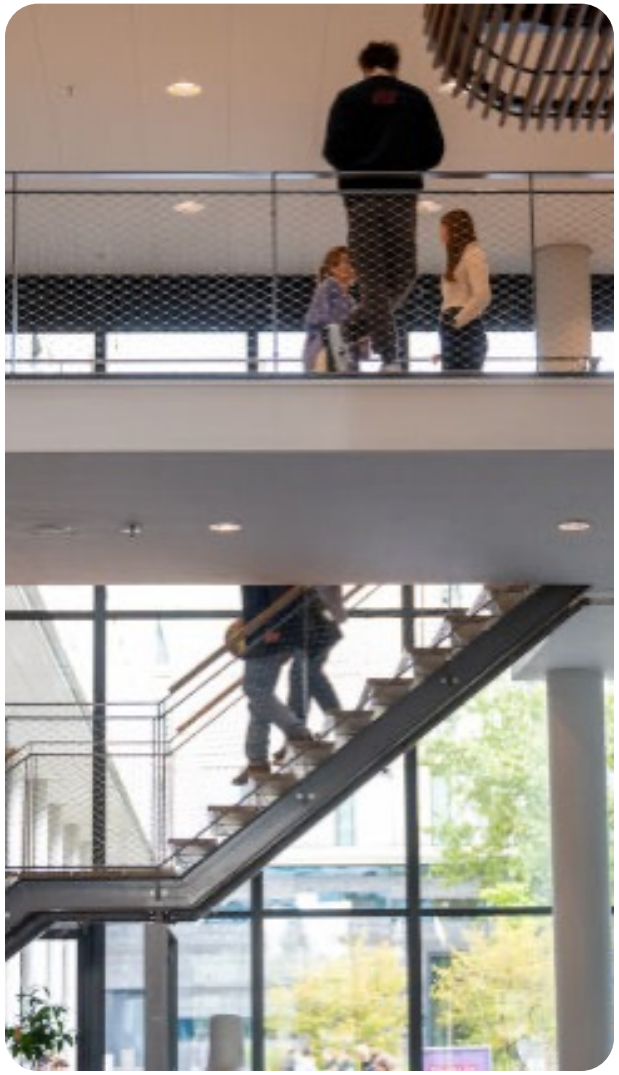
Voortvloeiende initiatieven

- Attack Surface Management (ASM)
  - openKAT
  - Open source tools
- Exposure Management
  - Darkweb fora / markets
  - Social media (Telegram)
- Dashboard
  - Samenbrengen van bevindingen
  - IV-metingen

SURF Dienstontwikkeling

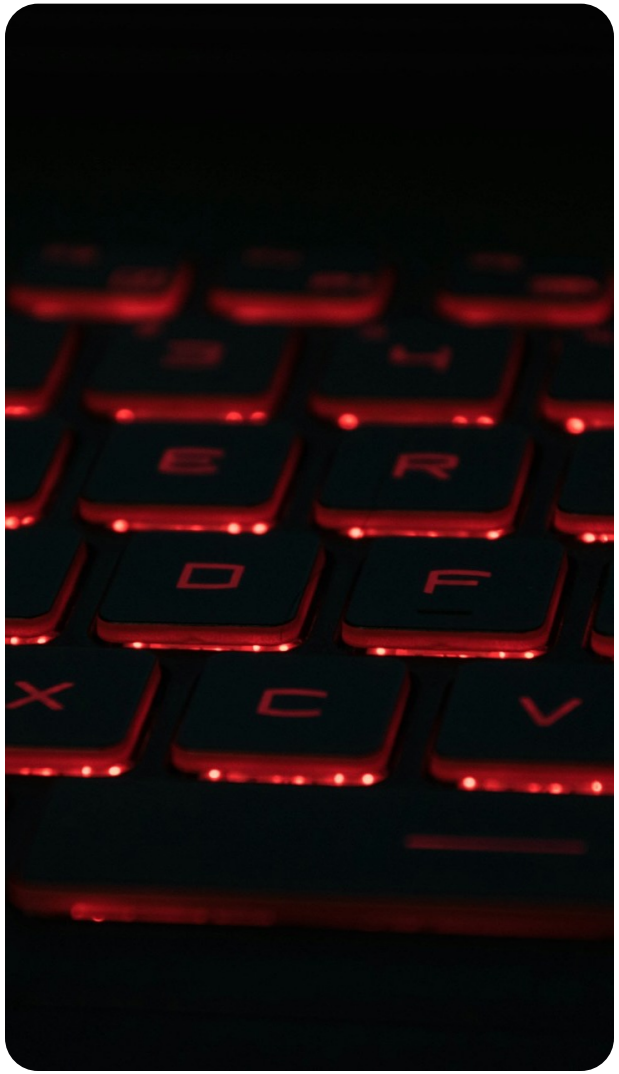
- In de SPA besproken als “BP 0.1 – Exploratie”
  - ‘van Check tot Hack’ als belangrijkste input
  - Getoetst bij HBO, WO CISO’s en SURF intern

- Eerder gepauzeerd door onduidelijke behoefte en weinig inhoudelijke kennis en ervaring
- Scope nu duidelijker:
  - Begeleiding en bijhouden van voortgang en bevindingen
  - Uitbreiden van eigen tooling/ervaring voor kleine testen
  - Professionaliseren van testmangerschap en dreigingsinformatie voor Red Teaming



ART-SURF Red Teaming Raamwerk

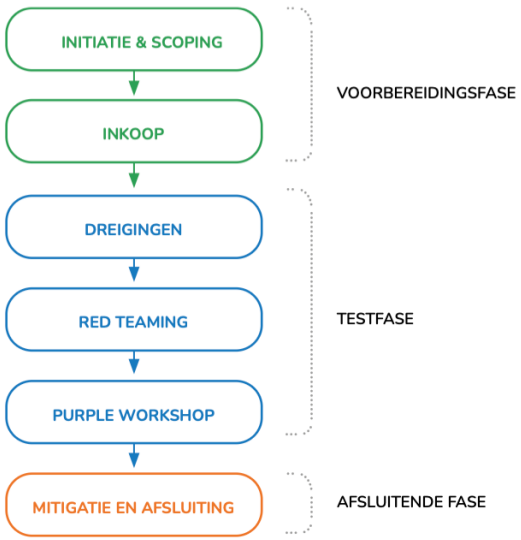
- Op basis van ART-NL, TIBER-NL, ZORRO en SURF's opgedane ervaringen
- Samen met Maarten Bras en twee klankbordgroepen vanuit SCI[PR, RT]
- Houvast en het borgen van kwaliteit tijdens inkoop, uitvoering en het delen van resultaten
- Een *best practice* die bekend is binnen de markt
- Basis voor testmanagerschap en threat intelligence door SURF



fase rekening te houden met gemiddeld zo'n 30-50% van de werktijd voor de Control Team Lead. Tijdens deze fase is het belangrijk dat de Control Team Lead andere taken kan laten vallen als dit nodig is voor de lopende test. Voorafgaand aan de Red Team fase en na afloop is de tijdsbesteding afhankelijk van de complexiteit van de inkoop en scoping en de bevindingen vanuit de test. Voor de overige leden van het Control Team zal de tijds-besteding minder zijn aangezien zij de Control Team Lead ondersteunen.

2.4 Belangrijkste stappen en mijlpalen

De ART-SURF-test omvat drie verschillende fasen: voorbereiden, testen en afsluiten. Binnen deze fasen zitten weer subfasen gekenmerkt door specifieke vereisten waaraan moet worden voldaan voordat naar de volgende fase kan worden overgegaan. Dit hoofdstuk biedt een overzicht van de verschillende stappen, de belangrijkste te behalen mijlpalen en de gemiddelde tijds-besteding voor elke fase.



VOORBEREIDINGSFASE

INITIATIE & SCOPING

Wat is het?
In de initiatie- en scopingfase werken het SURF-TCT en de Control Team Lead van de instelling samen om de parameters van de ART-SURF-test te bepalen. Dit omvat het identificeren van de leerdoelen van de instelling, het kiezen van de geschikte modules, het bepalen van de samenstelling van het Control Team, het plannen van de test, het beoordelen van het huidige niveau van cyberweerbaarheid en het bepalen of de instelling een volledig overzicht heeft van haar kritieke systemen en processen.

Mijlpalen
- Ondertekende overeenkomst tussen de bestuurder van de instelling en SURF voor test management en threat intelligence van SURF
- Oprichting van een Control Team
- Akkoord over de codenamen en communicatie-kanalen
- Ingevuld scopingsdocument
- De scope van ART-SURF wordt goedgekeurd door de sponsor op bestuursniveau van de instelling en SURF-TCT

Gemiddelde duur
4-6 weken

3 Organiseren

Dit hoofdstuk geeft een overzicht van de belangrijkste elementen die moeten worden voorbereid en georganiseerd voordat een instelling begint met een ART-SURF-test. Het bevat inzichten met betrekking tot riskmanagement, projectmanagement, rapportering en verantwoordelijkheden.

3.1 Overzicht van verplichte documentatie

Eén van de doelstellingen van ART-SURF is om verplichte documentatie zoveel mogelijk te beperken. Een lagere documentatielast voorkomt een onnodige belasting van Control Teams en Red Teams. Toch is een zekere mate van documentatie essentieel. Vooral omdat bepaalde (essentiële) rapporten en logboeken de basis vormen voor verbeteringen binnen de geteste instelling. De volgende documentatie moet worden voorzien tijdens of na de voltooiing van een ART-SURF-test:

Naam	Auteur	Doelstelling	Opleveren in fase
ART-SURF-overeenkomst	TCT en Control Team	De ART-SURF-overeenkomst beschrijft de verantwoordelijkheden van zowel het Control Team als SURF voor de ART-SURF-test.	INITIATIE & SCOPING
Scoping	Control Team	Een document dat de kritische functies, systemen en middelen identificeert die in de test zullen worden opgenomen. Het scopingdocument zorgt ervoor dat het Control Team, SURF-TCT en het Red Team een duidelijk inzicht hebben in de systemen en processen die van belang zijn, en dat ze binnen de vooraf bepaalde scope blijven.	SCOPING
TI-rapport	TI- analist	Een document dat het dreigingslandschap van de instelling beschrijft. Het identificeert ook online gevonden informatie, biedt een bedrijfsoverzicht en aanvalsscenario's. Op basis van deze informatie maakt het Red Team het Red Team-plan.	THREAT INTELLIGENCE
Red Team-testplan	Red Team	Een document waarin de TI-scenario's worden omgezet in een technisch aanvals-plan, compleet met technieken, tactieken en procedures (TTP's) en modus operandi van de geselecteerde dreigingsactoren (met behulp van MITRE ATT&CK). Bovendien moet het document beschrijvingen bevatten van mogelijke leg-ups, risicomanagement en de verwachte tijdlijn voor de uitvoering.	RED TEAMING
Red Team-rapport	Red Team	Een Red Team-rapport is een uitgebreid document met de bevindingen, waarnemin-gen en aanbevelingen van de Red Team-fase.	RED TEAMING

ART-SURF Red Teaming Raamwerk

Vers van de pers:

https://sec.surf.nl/asset/red-teaming-raamwerk/

Eerste pilots in ‘25-’26: Ben je al bezig? Wil je starten?
ART@surf.nl

edu.nl/gmwvr

mbo digitaal

Vragen?

m.deben@mbodigitaal.nl
joost.gadellaa@surf.nl