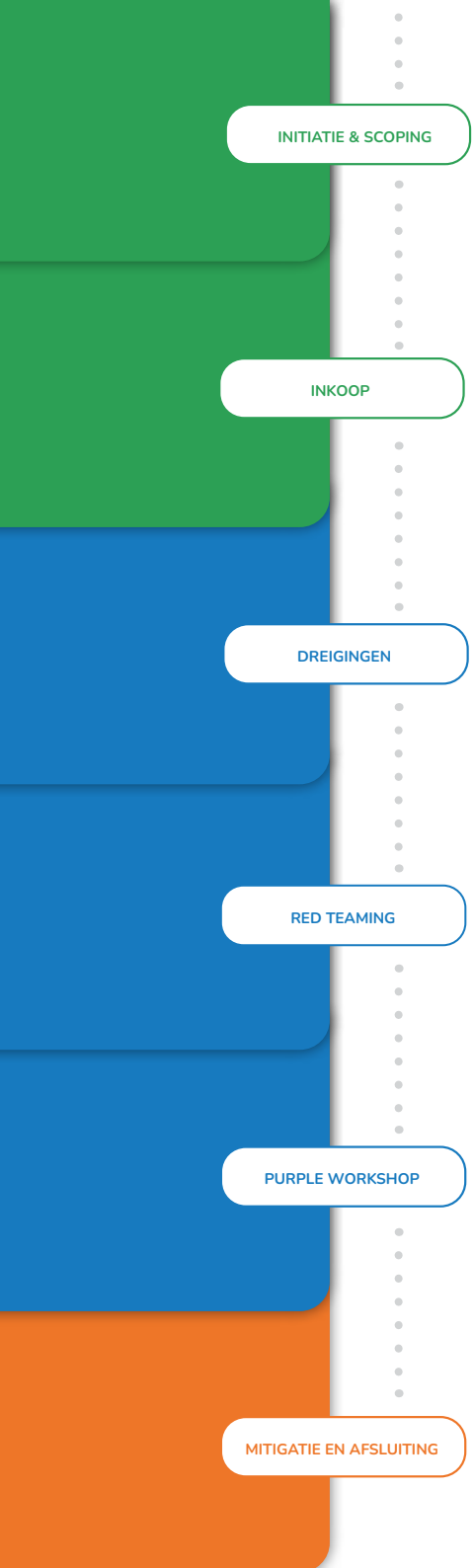


ART-SURF 1.0

Een gesimuleerde cyberaanval op onderwijs- en onderzoeksinstellingen, bedoeld om realistische dreigingen na te bootsen en daaruit te leren.

SURF

inhoud

1 Wat is ART-SURF?

ART-SURF is een gesimuleerde cyberaanval op onderwijs- en onderzoeksinstellingen, bedoeld om realistische dreigingen na te bootsen en daaruit te leren.

Incidenten binnen de onderwijs- en onderzoekssector laten zien dat digitale aanvallers onze sector weten te vinden. Deze aanvallen, van criminelen tot statelijke actoren, kunnen de continuïteit van onderwijs en onderzoek bedreigen. Met ART-SURF leer je van zulke dreigingen voordat ze écht plaatsvinden.

Red teaming is één van de manieren om te testen of toegepaste maatregelen effectief zijn en eventueel welke nieuwe maatregelen meerwaarde zouden hebben. Daarom heeft SURF, samen met haar leden, ART-SURF ontwikkeld. In deze red team-testen worden mensen, processen en systemen van leden getest met behulp van technieken en werkwijze van actuele dreigingsactoren die binnen en buiten onze sector actief zijn (geweest).
SURF zal haar leden begeleiden met testmanagers en een threat intelligence rapport om te garanderen dat de meest relevante technieken en hulpmiddelen van actuele dreigingen worden nagebootst in de red team test. Deze hulp komt vanuit het Test Cyber Team van SURF, hierna afgekort als SURF-TCT.

Het doel van Advanced Red Teaming-SURF (ART-SURF) is om de preventie, detectie en respons[1] van je instelling te testen en te verbeteren op basis van de testresultaten. Je personeel wordt niet vooraf op de hoogte gebracht van de test, behalve een klein team dat verantwoordelijk is voor de test het zogenaamde Control Team.

Is jouw instelling klaar voor red teaming en lid van SURF? Neem dan contact op met SURF via ART@surf.nl

1.1 Het ART-SURF-raamwerk

Op basis van ervaringen uit andere sectoren en enkele pilots binnen de eigen sector heeft SURF besloten om het Advanced Red Teaming Framework, aangeduid als ART, te gebruiken als de basis voor ART-SURF. ART is ontwikkeld door De Nederlandsche Bank in samenwerking met andere sectoren en op basis van de ervaringen met het red teaming raamwerk Threat Intelligence-Based Ethical Red-teaming (TIBER). Met meer dan 100 succesvolle TIBER red teaming testen in Europa, biedt ART een solide basis voor ART-SURF. SURF heeft ervoor gezorgd dat ART wordt aangepast voor een optimale werking in de onderwijs- en onderzoeksector. ART-SURF is er dan ook primair voor instellingen in de onderwijs- en onderzoeksector die niet al onderdeel zijn van een ander red teaming raamwerk.

1 https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

De afgelopen jaren heeft Threat Intelligence Based Ethical Red-teaming (TIBER) bewezen een effectieve tool te zijn om de cyberbeveiliging van individuele instellingen in de financiële sector en voor de sector als geheel te vergroten. SURF gelooft erin dat ART-SURF de cyberweerbaarheid van de onderwijs- en onderzoekssector zal vergroten en ervoor zal zorgen dat geleerde lessen worden gedeeld onder haar leden.

1.2 Wat is ART?

ART is een uitgebreid raamwerk dat een breed scala aan instellingen in staat stelt om geavanceerde red teaming tests uit te voeren, gebaseerd op threat intelligence van hoog niveau. Als een evolutie van het TIBER-raamwerk geeft ART deelnemende instellingen de vrijheid om verschillende modules te kiezen en aan te passen, om ervoor te zorgen dat elke test aansluit bij hun specifieke behoeften en leerdoelen.

Door instellingen in staat te stellen om modules te kiezen die het meest relevant zijn voor hun cyberbeveiliging, volwassenheidsniveau en beschikbare middelen, stelt ART hen in staat hun inspanningen en investeringen in cyberbeveiliging te optimaliseren. Deze aanpak resulteert in een aangepaste red teaming test die precies aansluit bij hun unieke leerdoelen. Het modulesysteem van ART biedt deelnemende instellingen flexibiliteit en waarde, wat de documentatievereisten vermindert terwijl de strenge testnormen voor cyberbeveiliging van TIBER-EU gehandhaafd blijven. Na succesvolle voltooiing van een test volgens dit raamwerk wordt het officieel geregistreerd als een ART-SURF-test.

1.3 Voor wie is ART-SURF bedoeld?

Hoewel een red team test een goede manier is om de cyberweerbaarheid van jouw organisatie te verbeteren, heeft je instelling een bepaalde mate van volwassenheid nodig om het de moeite waard te maken.

Basis op orde

Als je instelling nog veel basisaspecten van informatiebeveiliging op orde moet krijgen, is een red team test niet zinvol. Het is beter om eerst op deze basis te focussen en dan eerst de toegepaste maatregelen te testen met pentests en daarna een bredere test uit te voeren via red teaming[2,3].

Detectie en respons

Een red team test kijkt niet alleen naar de preventieve maatregelen die u hebt ingesteld, maar ook naar detectie en respons. Als u geen team heeft dat hier actief aan werkt (zoals een Security Operations Center (SOC))[4], is een andere oefening of test misschien geschikter. Bij gebruik van een extern SOC is het van belang dat je instelling intern ook opvolging kan geven aan eventuele bevindingen van dit SOC.

Leerervaring

Om zoveel mogelijk uit een red team test te halen, is het belangrijk dat je instelling bereid is om ervan te leren. Tijdens de gesimuleerde aanval zullen lessen worden geleerd. Systemen die anders ingesteld hadden moeten worden of medewerkers die niet de juiste procedure volgden. Het is belangrijk dat dit niet wordt bestraft, maar wordt gezien als een leerervaring. Ondersteuning van het bestuur is hierbij heel belangrijk zodat medewerkers zich gesteund voelen om zoveel mogelijk lering uit de test te halen.

Budget & personeel

Naast het budget voor het inhuren van een red team provider, moet u budget voorzien voor het opvolgen van bevindingen zoals hiervoor gesteld. Een red team test heeft weinig nut zonder een budget om aan deze resultaten te werken. Bovendien moet u tijd vrijmaken binnen de relevante teams om zicht te houden op de red team test. Ook hier is de ondersteuning van het bestuur cruciaal. Zij moeten de bevindingen en de opvolging serieus nemen en de noodzakelijke mensen en middelen hiervoor beschikbaar stellen.

2 Voor meer informatie over verschillende soorten testen en oefeningen kunt u ook de SURF keuzekaart cybersecurity-weerbaarheidstesten raadplegen via https://sec.surf.nl/keuzekaart-cybersecurity-weerbaarheidstesten/
3 Zie bijvoorbeeld https://www.ncsc.nl/wat-kun-je-zelf-doen/basisprincipes
4 SURF levert SOC-dienstverlening voor zijn leden https://www.surf.nl/diensten/surfsoc

1.4 Wat is het verschil tussen ART-SURF en normaal red teaming?

In vergelijking met 'normaal' red teaming en pentests heeft ART-SURF de volgende voordelen:

- Gegarandeerde aandacht van het bestuur als onderdeel van het raamwerk;
- Geteste systemen zijn live productiesystemen die je kritieke functies ondersteunen;
- ART-SURF-tests zijn altijd op basis van threat intelligence;
- Een hoog controleniveau wordt gegarandeerd door een SURF Test Cyber Team (SURF-TCT) ;
- De test volgt een bewezen raamwerk;
- ART-SURF is specifiek voor de onderwijs- en onderzoeksector;
- Jouw instelling leert van alle testen binnen de sector, dankzij gestructureerde kennisdeling via SURF

1.5 Doel van het raamwerk

Dit raamwerk is ontwikkeld door SURF in nauwe samenwerking met De Nederlandsche Bank, Z-CERT en andere relevante ART-deelnemers en is een afgeleide van het TIBER-EU-raamwerk. Het is bedoeld voor ART-SURF-deelnemers en hun providers. Het geeft uitleg over de belangrijkste fasen, activiteiten, op te leveren producten en interacties die onderdeel zijn van een ART-SURF-test voor de onderwijs- en onderzoeksector. Dit document is eerder een leidraad dan een gedetailleerde voorgeschreven methode. Daarom moet het samen met ander relevant ART-SURF-materiaal worden geraadpleegd, dat wordt voorzien door het SURF-TCT aan ART-SURF-deelnemers. Dit raamwerk geeft alleen details over het ART-SURF-testproces voor de onderwijs- en onderzoeksector. Het SURF-TCT staat ter beschikking om vragen te beantwoorden over het ART-SURF-testproces of het ART-SURF-programma.

1.6 Disclaimer en juridische informatie

De informatie en meningen in dit document zijn louter informatief. Ze zijn niet bedoeld als juridisch of ander professioneel advies en mogen niet worden gebruikt ter vervanging voor specifiek advies dat relevant is voor bepaalde omstandigheden. De sponsors en auteurs van dit document aanvaarden geen aansprakelijkheid voor eventuele fouten, weglatingen of misleidende verklaringen in dit document, of voor verlies dat kan voortvloeien uit het vertrouwen op de informatie en meningen die erin voorkomen.

2 ART-SURF overzicht

Het doel van dit hoofdstuk is om een overzicht te bieden van (1) de belangrijkste deelnemers die betrokken zijn in de test, (2) de belangrijkste stappen en mijlpalen in het ART-SURF-proces en (3) de verschillende beschikbare modules.

2.1 Belangrijkste deelnemers

Bij een ART-SURF-test zijn veel verschillende partijen betrokken, elk met hun eigen rol, taken en verantwoordelijkheden. De belangrijkste deelnemers en hun rollen zijn hieronder vermeld.

Testmanagers van het Test Cyber Team

Het Test Cyber Team bestaat uit de testmanagers en de Threat Intelligence Analist die ART-SURF-testen binnen de sector begeleiden. De rol van de Testmanagers van het SURF -Test Cyber Team (SURF-TCT) is om ervoor te zorgen dat instellingen op een uniforme en gecontroleerde manier worden getest, in overeenstemming met de vereisten van het ART-SURF-raamwerk. SURF benoemt de testmanagers voor elke test, die nauw samenwerken met het Control Team van de instelling tijdens het hele ART-SURF-proces. De Test-managers werken nauw samen met het Control Team, maar maken formeel geen deel uit van het team. Ze hebben het recht om grote afwijkingen van de scope of het scenario van de test te escaleren aan de programmamanager van ART-SURF, aan wie ze rechtstreeks rapporteren.

Threat Intelligence analist van het Test Cyber Team

De Threat Intelligence (TI)-analist van SURF vanuit het Test Cyber Team is verantwoordelijk voor het leveren van (gerichte) threat intelligence tijdens de testfase en verschaft, indien noodzakelijk, bijkomende informatie tijdens de Red Team-fase. Het belangrijkste product dat TI-analist levert is het Threat Intelligence-rapport, met een bedrijfsoverzicht, een dreigingslandschap voor de instelling, gerichte threat intelligence en mogelijke scenario('s).

Control Team

De Control Teamleden zijn de enige medewerkers van de instelling die volledig op de hoogte zijn van de test. Zij hebben de leiding over de test en kunnen deze te alle tijden pauzeren als ze risico's voorzien. Het Control Team bestaat uit een Control Team Lead en zijn verplichte vervanger, extra deskun-digen en, indien nodig, derde partijen. Indien mogelijk en gewenst kan de Control Team Lead een interne TI-expert betrekken in de TI-fase van de test om de TI-scenario's te verbeteren. Een sponsor vanuit het bestuur maakt ook deel uit van het Control Team. Deze persoon wordt regelmatig op de hoogte gebracht van de belangrijke ontwikkelingen door de Control Team Lead.

Bestuurder

De bestuurder is een belangrijke deelnemer gedurende de test. De bestuurder maakt deel uit van het Control Team en moet de formele toestemming geven om de test te starten. Deze 'sponsor op bestuursniveau' is strategisch geïnformeerd over de test. Indien nodig kan deze persoon beslissingen nemen over bepaalde gebeurtenissen tijdens de test. Het is de verantwoordelijkheid van de Control Team Lead om de bestuurder betrokken en op de hoogte te houden tijdens de test. De andere bestuursleden zijn niet op de hoogte van de test en dus alleen betrokken bij de afsluitingsfase. Tijdens deze fase wordt de test tijdens een bestuursvergadering besproken zoals toegelicht in 6.3.

Blue Team

Het Blue Team is het verdedigende team van de instelling, inclusief het Security Operations Center (SOC). Het Blue Team wordt pas op de hoogte gebracht van de test nadat deze voltooid is. Er kan zich echter een situatie voordoen waarin het Blue Team, toevallig of door goed werk, kennis krijgt van de test (of onderdelen ervan) voordat deze voltooid is. Na de testfase mag het Blue Team volledig op de hoogte worden gebracht van de test.
Het evalueert samen met het Red Team de bevindingen en creëert leerervaring tijdens de Purple workshop. Het Blue Team bestaat uit medewerkers die niet vooraf op de hoogte zijn van de test, zoals SOC-analisten, IT-beheerders en gebruikers die mogelijk doelwit zijn van simulaties zoals phishing.

Red Team

Het Red Team is verantwoordelijk voor het uitvoeren van het scenario-gebaseerde hacken van de ART-SURF-test, waarvoor het een team van technische experts moet voorzien. Er moet een Red Team Lead zijn en meerdere andere leden die gespecialiseerd zijn in verschillende gebieden van red teaming. De belangrijkste producten die het Red Team levert zijn het aanvalsplan en het testrapport van het Red Team. Het Red Team is ook verantwoordelijk voor het organiseren en leiden van de Purple workshop.

2.2 Rol van SURF

Binnen een ART-SURF test kan SURF als organisatie meerdere rollen hebben. Het is belangrijk om aan te geven dat deze duidelijk gescheiden zijn en communicatie tussen de rollen alleen plaatsvindt als dit in het ART-SURF proces geregeld is.

SURF stelt zoals hiervoor besproken vanuit het SURF-TCT twee Testmanagers aan voor de test en ook levert SURF een Threat Intelligence analist voor het Threat Intelligence Rapport. Daarnaast kan SURF als leverancier of Blue Team via SURFcert/SURFsoc betrokken zijn bij de test. In deze rol als leverancier of Blue Team zal SURF op dezelfde manier in het proces worden betrokken als andere vergelijkbare partijen. Dat betekent bijvoorbeeld dat het Blue Team van SURF niet geïnformeerd wordt over lopende testen.

2.3 De verantwoordelijkheden van het Control Team

De Control Team Lead is verantwoordelijk voor het beheer van het project en de risico's van de ART-SURF test. Dit betekent dat het onder andere verantwoordelijk is voor het plannen van verplichte bijeenkomsten, het maken van afspraken rond communicatiemethoden, codenamen, het bijhouden van risico's en het opstellen van een algemene planning op hoog niveau voor de hele test. Bij projectmanagement zorgt de Control Team Lead er ook voor dat interne belanghebbenden, zoals het bestuur, tijdig worden betrokken in de test, en dat de externe partijen volgens de planning leveren of dat de planning wordt aangepast bij wijzigingen. De planning moet worden opgesteld en gedeeld met alle betrokken partijen.

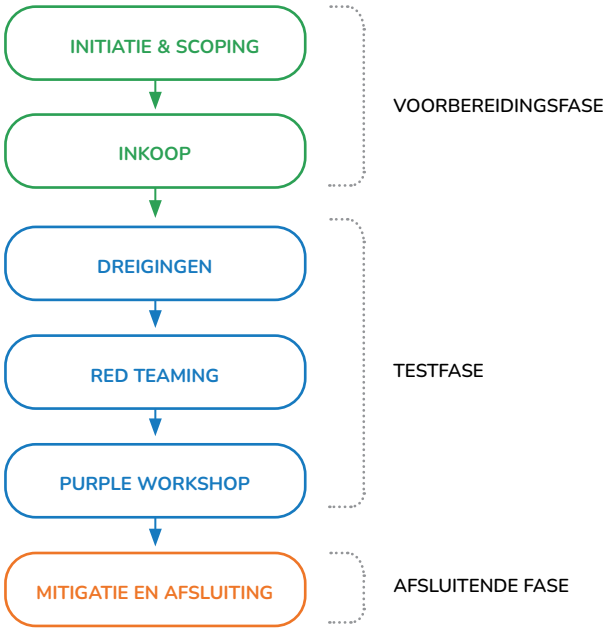
Gezien deze verantwoordelijkheden is het belangrijk dat de Control Team Lead ervaring heeft met projectmanagement en het communiceren met de verschillende lagen binnen de organisatie van technisch tot bestuursniveau.

Qua tijdsbesteding zal de Control Team Lead het meeste tijd kwijt zijn aan het organiseren van de test. Het is goed om tijdens de actieve Red Teaming

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 tijdsbesteding 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 tijdsbesteding 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 communicatiekanalen
- 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

VOORBEREIDINGSFASE

INKOOP

Wat is het?
In de inkoopfase vraagt de Control Team Lead offertes aan bij verschillende Red Team-providers voor de ART-SURF-test zoals bepaald tijdens de initiatie- en scopingfase. De duur van deze fase kan aanzienlijk variëren, vooral afhankelijk van de complexiteit van de inkoopprocedures van de instelling. Hoewel het scenario nog niet duidelijk is, start de instelling met de inventarisatie en het voorbereiden van leg-ups. Een leg up helpt het Red Team om alsnog een bepaalde positie te bereiken mocht dit hun niet binnen de gestelde tijd lukken. Je kunt hierbij bijvoorbeeld denken aan toegang tot een bepaald systeem.

Mijlpalen
- Succesvolle inkoopprocedure op basis van de testvereisten
- Ondertekende overeenkomst tussen de instelling en het Red Team
- Leg-up inventarisatie en voorbereiding

Gemiddelde duur
6-8 weken

TESTFASE

DREIGINGEN

Wat is het?
In deze fase formuleert de TI-analist van SURF één of meerdere scenario's op basis van dreigingen die de basis vormen voor het Red Team-plan en de uitvoering. De scenario's bestaan uit 3 fasen: In, Through en Out. De aanvaller moet binnenkomen, beweegt zich dan door het netwerk en voert uiteindelijk het eindoel uit in de Out-fase.

Mijlpalen
- Succesvolle 'go-bijeenkomst', die de start van de ART-SURF-test formaliseert
- Een 'business overview workshop' waarin de instelling informatie verstrekt over haar kritieke IT- en bedrijfsprocessen, doelstellingen en andere relevante ontwikkelingen aan de TI analist en het Red Team
- Succesvolle opzet (en goedkeuring) van het control team van één of meer op TI gebaseerde scenario's die als basis dienen voor het Red Team-plan
- Oplevering van het Threat Intelligence rapport vanuit SURF
- Een go/no go op het Threat Intelligence-rapport van SURF

Gemiddelde duur
Tussen 3 en 6 weken

TESTFASE

RED TEAMING

Wat is het?
In deze fase zet de Red Team-provider de threat intelligence scenario's om in een praktisch Red Team-plan, gestructureerd volgens het MITRE ATT&CK-raamwerk. Zodra de sponsor uit het bestuur en de Control Team Lead het Red Team-plan definitief hebben goedgekeurd, gaat het Red Team over tot het uitvoeren van het werkelijke hacking-onderdeel van de test. De duur van deze fase varieert op basis van de specifieke modules die zijn gekozen voor de red teaming test.

Mijlpalen
- Oplevering van het Red Team-plan
- Een go/no go op het Red Team plan
- Behalen van gestelde vlaggen tijdens de red teaming fase
- Oplevering Red Team-rapport
- Oplevering Blue team tijdlijn en acties

Gemiddelde duur
Tussen 6 en 12 weken

TESTFASE

PURPLE WORKSHOP

Wat is het?
Bij de Purple workshop werken het Red en Blue Team, na het afronden van de actieve testfase, samen om inzichten, zwakke punten en aanvalspaden te delen die tijdens de test zijn gebruikt of ontdekt. Het doel van deze samenwerking is om de beveiligingspositie van de instelling te verbeteren. De duur van de Purple workshop hangt af van de gekozen Purple Teaming module. De workshop bestaat uit een replay waarin het Red en Blue Team de uitgevoerde scenario's stap voor stap bespreken en daarna wordt samen verder gekeken welke acties het Blue Team het meeste zouden helpen om zoveel mogelijk van de Red Team test te leren.

Mijlpalen
- Uitvoering van de Purple workshop met het Blue en Red Team
- Oplevering definitieve versie van het Red Team rapport

Gemiddelde duur
Ongeveer 2 weken

AFSLUITENDE FASE

MITIGATIE EN AFSLUITING

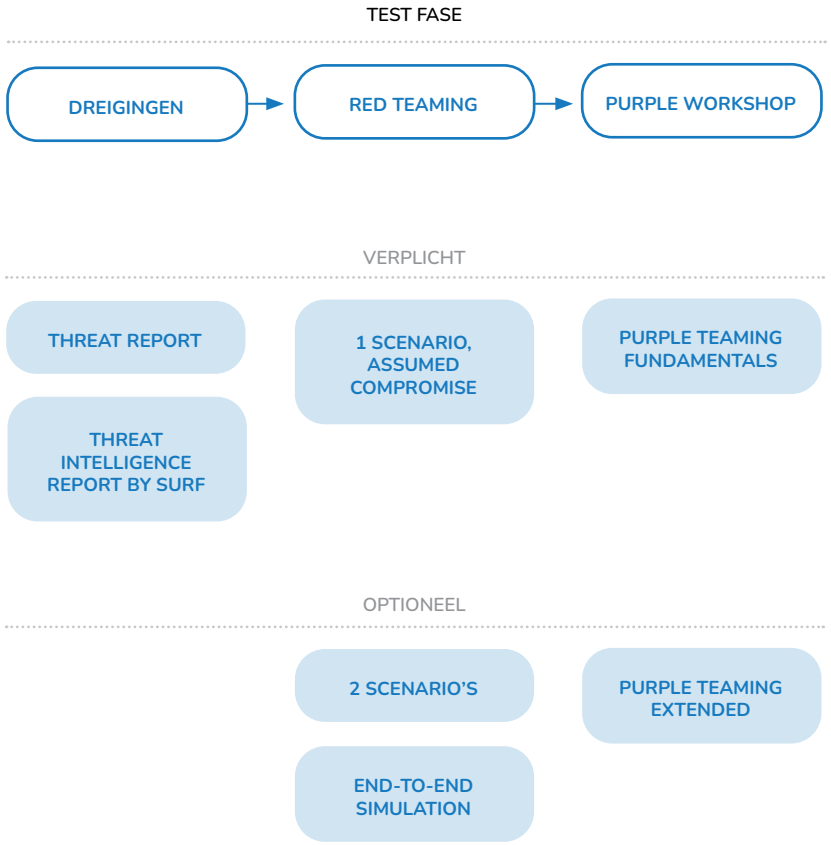
Wat is het?
De mitigatie- en afsluitingsfase is de laatste fase van de ART-SURF-test, waarin de instelling begint met het implementeren van een plan om de lessen die tijdens de ART-SURF-test zijn vastgesteld, aan te pakken en op te lossen. Bovendien worden alle relevante documenten geformaliseerd en wordt het ART-SURF-proces geëvalueerd tijdens een feedbacksessie. In deze sessie wordt het proces van de test geëvalueerd en geeft iedereen feedback op elkaar. Als laatste worden de lessen gedeeld met de andere instellingen om zo iedereen te laten leren.

Mijlpalen
- Een feedbacksessie
- Mitigatieplan
- Delen van de bevindingen

Gemiddelde duur
Ongeveer 2 weken

2.5 Belangrijkste verplichte en optionele modules

ART-SURF biedt meerdere verplichte en optionele modules. Dit hoofdstuk geeft een algemeen overzicht van deze modules.



Waarom zijn er verplichte en optionele modules?

Sommige onderdelen van de ART-SURF-test zijn verplicht om ervoor te zorgen dat de test voldoet aan de minimumeisen. Naast deze verplichte modules kunnen instellingen kiezen uit verschillende optionele modules om de ART-SURF-test aan te passen aan hun budget, leerdoelen en volwassenheid. Op deze manier krijgt de instelling maximale leerwaarde voor haar investering.

Wie kiest de modules?

In de eerste fasen van een ART-SURF-test, vóór de inkoop, komen de Control Team Lead van de instelling en het SURF-TCT samen om een aantal zaken te bespreken (zie hoofdstuk 3). Een belangrijk onderwerp is de scope van de ART-SURF-test. Welke optionele modules moeten worden opgenomen hangt af van een aantal factoren, zoals vermeld in de vorige paragraaf. Hoewel de instelling uiteindelijk zelf beslist over welke modules worden opgenomen, is de weg die naar deze beslissing leidt een samenwerking tussen de Control Team Lead en het SURF-TCT. De volgende factoren spelen een rol in dit proces:

- De grootte van de instelling;
- Het budget van de instelling;
- De eerdere ervaring van de instelling met pentesten en red teaming;
- De leerdoelen van de instelling;
- De frequentie van de test.

Uit welke modules kunt u kiezen?

De optionele modules maken allemaal deel uit van de testfase. Ze omvatten de volgende stappen: threat intelligence, red teaming en Purple Teaming. In dit hoofdstuk wordt elk van deze stappen beschreven, samen met de beschikbare modules en hun belangrijkste doelstellingen.

Threat intelligence modules

In de threat intelligence fase (TI-fase), levert de threat intelligence analist van SURF aan het Control Team en het Red Team het meest recente dreigingsrapport en een instelling-specifiek threat Intelligence rapport met het/de meest waarschijnlijke scenario('s).

Verplicht:

- **Gebruik van het dreigingsrapport**
  Het jaarlijkse Cyberdreigingsbeeld onderwijs en onderzoek beschrijft de belangrijkste dreigingen voor de Nederlandse onderwijs- en onderzoek-sector. Deze publicatie wordt gedeeld met de SURF-leden en leveranciers van ART-SURF-tests.
- **Target intelligence en scenario('s) geproduceerd door TI-analist**
  Naast het jaarlijkse dreigingsrapport biedt SURF een Targeted Threat Intelligence Report. Dit rapport beschrijft de belangen en het dreigings-landschap voor de instelling en welke informatie er online gevonden kan worden door dreigingsactoren. Dit alles wordt samengebracht in meerdere scenario's waaruit de instelling kan kiezen en de basis is voor het Red Team bij het opstellen van het Red Team-plan.

Red teaming modules

In de red teaming fase (Red Team-fase) simuleert de red team provider een op dreigingsinformatie-gebaseerde aanval op een specifiek doel (systemen en diensten die één of meer kritische functies ondersteunen). De Red Team-fase is het belangrijkste onderdeel van een ART-SURF-test en is niet optioneel. Organisaties kunnen echter de intensiteit kiezen die volgens hen het beste past door zowel het aantal scenario's als de duur van de test aan te passen.

Als de beschikbare tijd en middelen beperkt zijn, of als het opgegeven leerdoel dit vereist, is het mogelijk om één van de klassieke in-through-out-fases over te slaan met een goede rechtvaardiging. Hierdoor kan men de beschikbare tijd en middelen focussen op het onderdeel waar de instelling het meeste kan leren. De 'In-fase' kan bijvoorbeeld worden overgeslagen door de provider een account of een laptop met toegang tot het netwerk te geven.

De Red Team-fase van een ART-SURF-test moet ten minste 6 weken duren voor één scenario, of 10-12 weken voor twee of meer scenario's. Het Control Team beslist samen met de Testmanagers van SURF de geschikte duur voor de instelling.

Verplicht:

- **Eén scenario en 'assumed compromise' als startpunt**
  De meest eenvoudige, en daarom verplichte, optie voor de Red Team-fase is een test die één scenario bevat en begint met 'assumed compromise', waardoor bijvoorbeeld de In-fase van de test wordt overgeslagen. De focus van de test ligt dan vooral op de andere fasen (Through en Out). Deze optie bespaart tijd en kosten, maar mist mogelijk waardevolle inzichten die opgedaan hadden kunnen worden in de In-fase. Als de In-fase wordt over-geslagen krijgt het Red Team een beginpunt zoals een laptop met account of andere login om vanuit daar de aanval te beginnen. Hierdoor mist het

Blue Team sporen voor het traceren hoe de actor binnen is gekomen. Ook is er hierdoor geen compleet verhaal te presenteren waardoor de urgentie mogelijk niet hetzelfde wordt ervaren.

Optioneel:

- **Twee scenario's**
  Als er meerdere dreigingsactoren zijn die een instelling kunnen aanvallen, is het nuttig om twee (of zelfs meer) aanvalsscenario's in één test te simuleren. Bijvoorbeeld een aanval door een criminele organisatie en door een statelijke actor. Daarvoor bestaat de optie om meer dan 1 scenario te spelen in de red teaming fase. Het is belangrijk om ervoor te zorgen dat deze scenario's aanzienlijk verschillen en een breed scala aan technieken, tactieken en procedures (TTPs) omvatten. Het is kostenefficiënter om twee scenario's te testen in één test dan om twee aparte tests uit te voeren.

End-to-end-simulatie

In plaats van het 'assumed compromise' als startpunt te gebruiken en de in-fase over te slaan, kan de instelling de aanval intensiveren door de volledige aanvalsketen te simuleren van begin tot eind (ook end-to-end- of In-Through-Out-simulatie genoemd). Dit kan helpen bij de identificatie van potentiële zwakke punten in de processen en beveiligingssystemen van de instelling, die mogelijk over het hoofd worden gezien bij 'assumed compromise'. Hierdoor kan de instelling nauwkeuriger haar grootste beveiligingsrisico's identificeren.

Scenario X

Een scenario X kan worden opgenomen naast de geplande scenario('s). Het doel van een scenario X is om aanvallen na te bootsen die in de nabije toekomst kunnen worden verwacht. Dit scenario kan zijn gericht op innovatieve technieken en tactieken en kan rekening houden met geopolitieke en maatschappelijke ontwikkelingen of ontwikkelingen in het dreigingslandschap die zal in de toekomst gevolgen hebben voor de instelling. Scenario X maakt gebruik van bevindingen van de eerdere scenario's en wordt daarom ontwikkeld tijdens de Red Team-fase. Het uiteindelijke doel van een Scenario X is gericht op een kritische functie, vaak met een zeer creatieve aanpak. Het gebruik van een scenario X wordt besloten en goedgekeurd door het Control Team en SURF-TCT halverwege de test.

Purple workshop modules

De Purple workshop wordt gewoonlijk uitgevoerd nadat de Red Team-fase van een test is voltooid. Als de omstandigheden van de Red Team-fase hierom vragen, kan de Purple Teaming-fase vroeger starten. Het is geen losse Purple teaming-test, maar een workshop op basis van de geleerde lessen uit de red teaming fase. Tijdens de Purple Teaming-fase komen het Red Team en het Blue Team namelijk samen om de stappen die het Red Team tijdens de test heeft genomen te doorlopen en om de door het Blue Team genomen (of niet genomen) maatregelen te bespreken. Het doel van deze sessie is om een beter inzicht te krijgen in de technieken en aanpak van elk team en om eventuele zwakke punten in de defensie van de instelling te identificeren en verbeteren. Ook kunnen meer procesmatige elementen die uit de test gekomen zijn ter sprake komen indien van toepassing.

Verplicht:

- **Purple workshop: basis**
  De meest eenvoudige, en daarom verplichte, optie voor de Purple Teaming-fase is een Purple workshop van één dag. Tijdens de Purple Teaming-basis delen het Red Team en Blue Team hun kennis, bekijken ze de gesimuleerde aanvallen en analyseren ze de bevindingen. Als er tijd is stellen ze ook manieren voor om de verdediging van de instelling te verbeteren. De Purple Teaming-basis optie is geschikt voor ART-SURF-tests met een relatief compacte Red Teaming-fase.

Optioneel:

- **Purple workshop: uitgebreid**
  De uitgebreide optie voor de Purple Teaming-fase is een Purple workshop van minimaal 2 dagen. De extra tijd kan ingezet worden om bepaalde paden van de Red Teaming fase opnieuw door te lopen of ongebruikte paden uit te lopen om zo de verdediging van de instelling te verbeteren.

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 aanvalsplan, 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, waarnemingen en aanbevelingen van de Red Team-fase.	RED TEAMING

3.2 Belangrijke bijeenkomsten

Dit is een gedeeltelijk overzicht van de belangrijkste bijeenkomsten tijdens een ART-SURF-test. Sommige bijenkomsten kunnen samengevoegd worden (bij business overview workshopVoor een complete lijst van bijeenkomsten kunt u hoofdstukken 4, 5 en 6 raadplegen

Naam	Deelnemers	Doelstelling
Pre-launch bijeenkomst	SURF-TCT en Control Team	Bijeenkomst vóór de formele start van de ART-SURF-test tussen het Control Team en het SURF-TCT waarin de scope, modules en andere fundamentele vereisten worden besproken.
Scoping- bijeenkomst	SURF-TCT incl. TI-Analist, Control Team, een bestuurder en Red Team	Tijdens de (laatste) scopingbijeenkomst wordt het scopingdocument goedgekeurd door de sponsor op bestuursniveau van de instelling en het SURF-TCT.
Launch- bijeenkomst	SURF-TCT incl. TI-analist, Control Team en Red team	Formele launch van de ART-SURF-test. Tijdens de launch-bijeenkomst worden volgende onderwerpen besproken: Het ART-SURF-proces en documentatie, deelnemers, rollen, verantwoordelijkheden en projectplanning. Het einde van deze bijeenkomst markeert de formele start van de ART-SURF-test.
Business overview workshop	SURF-TCT incl. TI analist, Control Team en Red Team	Workshop gegeven door een bedrijfsexpert van de instelling om het Red Team en TI-Analist te ondersteunen in het begrijpen van de instelling, haar processen en belangen.
Go/no go TI-rapport	SURF-TCT incl. TI analist, Control Team en Red Team	Nadat de TI-analist het TI-rapport heeft afgeleverd, wordt een bijeenkomst gehouden waarin het rapport formeel wordt goedgekeurd.
Go/no go Red Team-plan	SURF-TCT, Control Team en Red Team	Nadat het Red Team een aanvalsplan heeft opgesteld, wordt een bijeenkomst gehouden om het aanvalsplan formeel goed te keuren en de Red Team-fase van de test te starten.
Wekelijkse update-bijeenkomsten tijdens de Red Team-fase	SURF-TCT, Control Team en Red Team	Tijdens de testfase zijn er wekelijkse update-bijeenkomsten waarin het Red Team een update geeft over de voortgang in de voorbije week. De activiteiten voor de komende week worden ook besproken.
Purple workshop	Control Team, Red Team *Optioneel:* SURF-TCT	De Purple workshop start met een replaysessie, waarin het Red Team chronologisch door de uitgevoerde acties van de test gaat. Daarna werken het Blue Team en het Red Team samen op de gebieden met de meeste leerdoelen
Bestuursvergadering	Red Team, Control Team en bestuur *Optioneel:* SURF-TCT incl. TI-Analist	Na de Purple workshop en het finaliseren van het Red Team-rapport, wordt de test tijdens een bestuursvergadering besproken om de resultaten en de impact van de test te communiceren.
Feedbacksessie	SURF-TCT incl. TI-analist, Control Team, Red Team	Tijdens de feedbacksessie evalueren alle actief betrokken partijen de test. Het onderwerp van de evaluatie is het ART-SURF-proces, niet de testresultaten.

3.3 Risicobeheer

Een ART-SURF-test brengt altijd potentiële risico's met zich mee. Dit komt door de kritische rol van de systemen, mensen en processen waarop getest wordt. Het raamwerk en het bijbehorende proces zorgen dat een dergelijke test gecontroleerd kan worden uitgevoerd.

Risico's in kaart brengen en verminderen

Voordat een instelling een ART-SURF-test uitvoert, moet ze een grondige risicoanalyse uitvoeren van alle systemen die binnen de scope van de test kunnen vallen om ervoor te zorgen dat er back-ups zijn en eventuele schade kan worden hersteld. Bovendien moet de instelling de risico's van een ART-SURF-test beoordelen, deze in overweging nemen en effectieve risicobeperkende maatregelen nemen.

Een dergelijke risicobeoordeling moet minstens de volgende risico's in overweging nemen:

- Contractuele relatie met de Red Team provider en vertrouwelijkheid van informatie
- Reputatieschade bij schending van vertrouwelijkheid of onethisch gedrag
- Escalatie van crises en incidenten
- Operationele red teaming
- Operationele verdediging
- Opruimen na voltooiing van de test

Bij het inhuren van een Red Team provider zorgt de instelling ervoor dat er een onderlinge overeenkomst is over ten minste de volgende aspecten: de scope van de test, grenzen, timing en beschikbaarheid van de provider, contracten, te ondernemen acties en aansprakelijkheid (inclusief verzekering, indien van toepassing).

Daarnaast zorgt de betrokkenheid van de Testmanagers in de ART-SURF-test ervoor dat de test verloopt volgens de overeengekomen test scope, het scenario, de planning en het proces.

Risico's worden ook beperkt door een goede planning, het informeren van slechts een beperkte groep mensen in het hoger management over de test en de scope ervan en een duidelijke definitie van de scope en vooraf bepaalde escalatieprocedures. Het is belangrijk om op te merken dat de instelling de controle blijft houden over en verantwoordelijkheid blijft voor de test. Het Control Team kan de test op elk moment (tijdelijk) opschorten als er zorgen zijn over (potentiële) schade aan een systeem of bedrijfsproces. Vertrouwde contactpersonen binnen het Control Team die bovenaan de escalatieketen voor beveiligingsincidenten staan, helpen voorkomen dat miscommunicatie en kennis over de ART-SURF-test uitlekken.

Ethische grenzen

Een ART-SURF-test moet de huidige en mogelijk toekomstige acties van een echte dreigingsactor nabootsen. ART-SURF zou ook hetzelfde soort 'creatief denken' moeten gebruiken die dreigingsactoren zouden gebruiken – tot op zekere hoogte – om de test zo realistisch mogelijk te maken. Ondanks deze doelstelling zijn er bepaalde soorten gedrag die strikt verboden zijn in ART-SURF:

- Ongeoorloofde vernietiging van apparatuur;
- Ongeoorloofde wijziging van gegevens/programma's;
- Ongeoorloofd in gevaar brengen van de continuïteit van kritieke diensten;
- Afpersen, bedreigen of omkopen van medewerkers;
- Het betalen voor gestolen informatie;
- Het gebruik van namen, logo's of anderszins identificeerbare informatie van echte personen of bedrijven namens wie het control team geen toestemming kan geven.

Codenamen

Om lekkage van gevoelige informatie te voorkomen moeten codenamen worden gebruikt. Deze codenamen moeten zo goed mogelijk worden gebruikt in alle documenten die betrekking hebben op de ART-SURF-test, maar in ieder geval in documenttitels en in de documenten zelf. Elementen waarvoor geen codenamen kunnen worden gebruikt (zoals URL's en screenshots) zijn vrijgesteld en mogen de volledige naam van de instelling bevatten. Het SURF-TCT zal een codenaam toekennen aan elke unieke test. Deze codenaam wordt gebruikt in alle communicatie en documentatie tussen de partijen die in de test betrokken zijn. Naast deze codenaam kan de provider en/of de instelling hun eigen codenamen gebruiken voor interne communicatie.

Escalatie en het pauzeren of stoppen van de test

De test kan een niveau van escalatie bereiken waardoor het Blue Team relevante autoriteiten informeert, zoals de politie, inlichtingendiensten of gegevensbeschermingsinstanties. Het Control Team moet dit altijd proberen te voorkomen zodat externe partijen niet worden belast door een ART-SURF-test. Als het Control Team wordt geïnformeerd over een actieve escalatie naar externe autoriteiten, moet de test onmiddellijk worden gepauzeerd zodat maatregelen kunnen worden genomen om te voorkomen dat deze autoriteiten betrokken raken.

Persoonlijke identificeerbare informatie

Het is de taak van de instelling om contractuele afspraken te maken met het Red Team over, bijvoorbeeld, de privacy van hunmedewerkers. In geen geval mag privacy-gerelateerde informatie worden opgenomen in testrapporten.

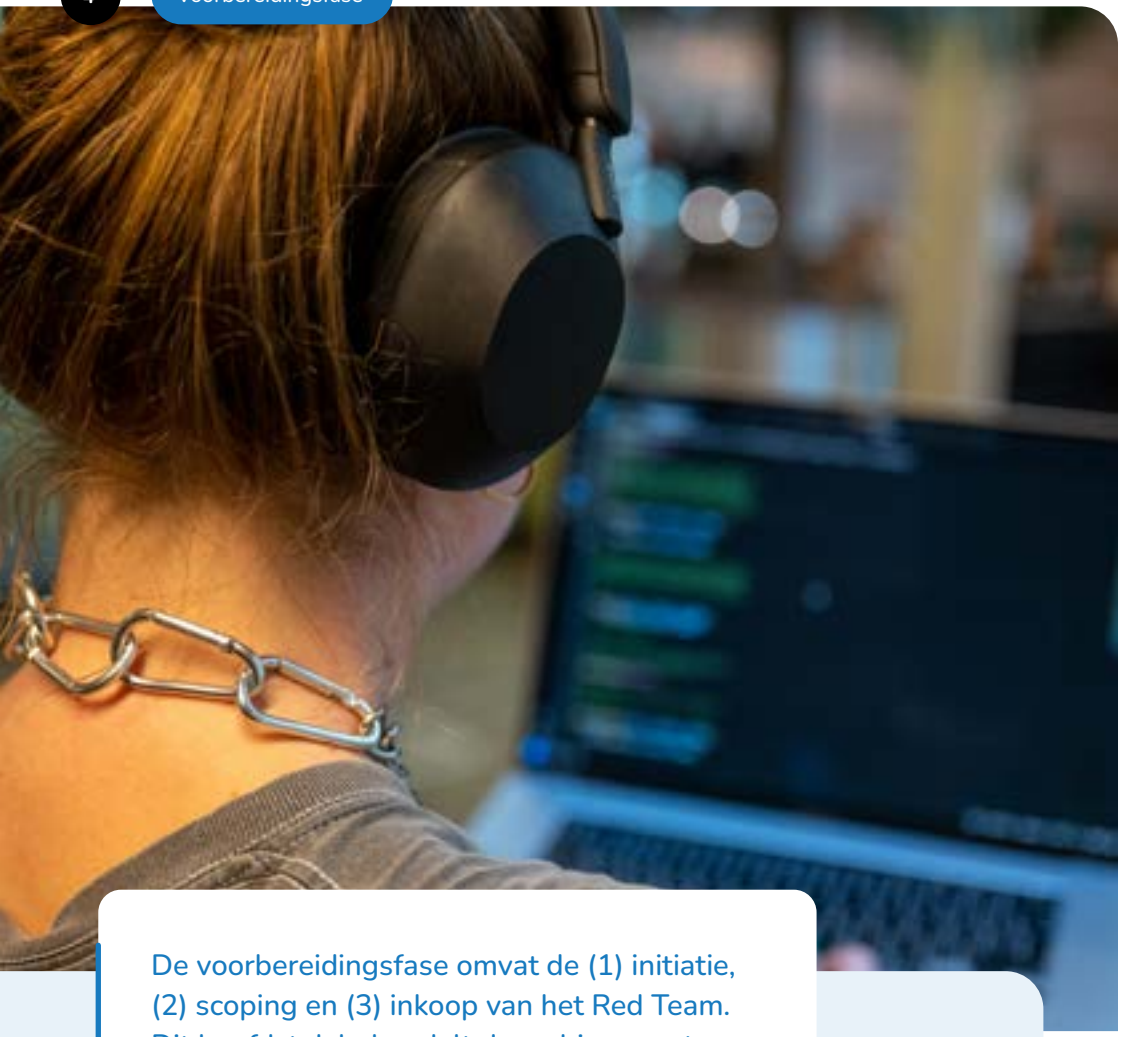
3.4 De test stoppen en/of het ART-SURF-label verwijderen

Aangezien het SURF-TCT niet betrokken is bij de commerciële relatie tussen het Red Team en de instelling, kan zij de test niet stoppen. Het heeft echter wel de bevoegdheid om het ART-SURF-label te verwijderen, wat betekent dat de test niet wordt erkend als een officiële ART-SURF-test. Het SURF-TCT moet terughoudend zijn bij de beslissing om het ART-SURF-label te verwijderen, rekening houdend met de kwaliteit en veiligheid van de test. Een beslissing om het label te verwijderen moet altijd worden genomen in overleg met de Control Team Lead, tenzij de situatie dit niet toelaat.

Het SURF-TCT kan het ART-SURF-label in ieder geval in de volgende situaties verwijderen:

- Het Red Team heeft (herhaaldelijk) aangetoond dat hij niet kan voldoen aan de normen van het ART-SURF-raamwerk en/of het vertrouwen van het SURF-TCT en/of Control Team heeft verloren om zijn taken uit te voeren op een gecontroleerde manier die past bij de delicate aard van de geheime test;
- De test is gecompromitteerd door het Red Team of de instelling, hetzij opzettelijk of als gevolg van (grove) nalatigheid;
- Als er sprake is van vals spel door het Control Team of Blue Team zoals het delen van informatie over de lopende test;
- Andere situaties die de kwaliteit, veiligheid of geheimhouding van de test in gevaar brengen.

Als het SURF-TCT beslist om het ART-SURF-label te verwijderen, dan kan de instelling ervoor kiezen om de test voort te zetten voor leerdoeleinden, of het kan het SURF-TCT raadplegen over de stappen die genomen moeten worden om ART-SURF-erkenning te verkrijgen.



De voorbereidingsfase omvat de (1) initiatie, (2) scoping en (3) inkoop van het Red Team. Dit hoofdstuk behandelt deze drie aspecten van de voorbereidingsfase.

4 Voorbereiding

4.1 Initiatiefase

Het belangrijkste doel van de initiatiefase is om de leerdoelen van de instelling en de scope van de test te bepalen, en het verkrijgen van toezegging van alle betrokken partijen. Tijdens deze fase bepalen het SURF-TCT en de Control Team Lead ook welke modules er zullen worden opgenomen in de test. Een ander doel van deze eerste fase is dat de instelling ervoor zorgt dat alle relevante interne belanghebbenden bij de ART-SURF-test betrokken zijn en op elkaar afgestemd zijn. De instelling zorgt er ook voor dat het SURF-TCT betrokken is. Onder begeleiding van het SURF-TCT kan de instelling beginnen met het opzetten van de ART-SURF-test. Tijdens deze fase kunnen het SURF-TCT en de Control Team Lead de ART-SURF-checklist gebruiken om te bepalen of alle vereiste stappen om een ART-SURF-test formeel te starten voltooid zijn. Al het bovenstaande wordt besproken tijdens een bijeenkomst (of meerdere bijeenkomsten) vóór de launch, de eerste officiële bijeenkomst van de ART-SURF-test. Tijdens deze bijeenkomst vraagt het SURF-TCT aan de Control Team Lead om een Control Team op te richten, bestaande uit een beperkt aantal senior medewerkers die de vereiste expertise hebben en/of deel uitmaken van de escalatieketen voor beveiligingsincidenten. De Control Team Lead zorgt ervoor dat ze op de hoogte zijn van de ART-SURF-test, de noodzaak van geheimhouding en het proces dat het team moet volgen als het Blue Team een ART-SURF-gerelateerd incident ontdekt en escaleert.

Bijeenkomsten
- Pre-launch bijeenkomst

Mijlpalen
- Ondertekende overeenkomst tussen SURF en de instelling;
- Oprichting van een controleteam;
- Akkoord over codenamen en communicatiekanalen;
- De scope van ART-SURF wordt goedgekeurd door de sponsor op bestuursniveau van de instelling.

4.2 Scoping

Kritieke functies binnen ART-SURF zijn gedefinieerd als:
"Kerntaken of activiteiten van een instelling die wanneer verstoord in termen van beschikbaarheid, integriteit of vertrouwelijkheid een serieuze impact hebben op de doelen van de instelling, de bredere sector of de Nederlandse samenleving." [5]

Organisaties in de onderwijs- en onderzoeksector ondersteunen en leveren deze functies op verschillende manieren via hun eigen interne processen, die worden ondersteund door kritieke systemen. Het zijn deze kritieke systemen, processen en de mensen hierin betrokken die de focus zijn van ART-SURF threat intelligence en red teaming. In het scopingdocument van ART-SURF worden vlaggen geplaatst op de kritieke systemen. Deze vlaggen zullen later dienen als doelstellingen in de testscenario's, die gebaseerd zijn op relevante threat intelligence. Tijdens het scopingproces moet de instelling het scopingdocument van ART-SURF invullen. Naast het bepalen van de scope, bevat het scopingdocument een lijst met de belangrijkste systemen en diensten die elke Kritische Functie ondersteunen. Deze informatie helpt het Control Team bij het plaatsen van de 'vlaggen' die moeten worden vastgelegd, die in wezen de doelen en doelstellingen zijn die het Red Team moet nastreven tijdens de test. Het Control Team bespreekt de vlaggen met de Testmanagers. Hoewel de vlaggen worden ingesteld tijdens het scopingproces, kunnen ze in sommige gevallen worden gewijzigd, op basis van threat intelligence en naarmate de test evolueert. Als externe partijen betrokken zijn bij het leveren van de beschreven kritische functies moet dit vermeld worden in het scopingdocument. In overleg met de Testmanagers kan dan besloten worden of en wanneer deze partijen geïnformeerd moeten worden. Aangezien niet de volledige scope zoals vermeld in het scopingdocument getest wordt kan het zijn dat de leverancier geen onderdeel van de test wordt.

Bijeenkomsten
- Scopingbijeenkomst(en)

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 communicatiekanalen
- Ingevuld scopingsdocument
- De scope van ART-SURF wordt goedgekeurd door de sponsor op bestuursniveau van de instelling.
- Leg-up inventarisatie en voorbereiding

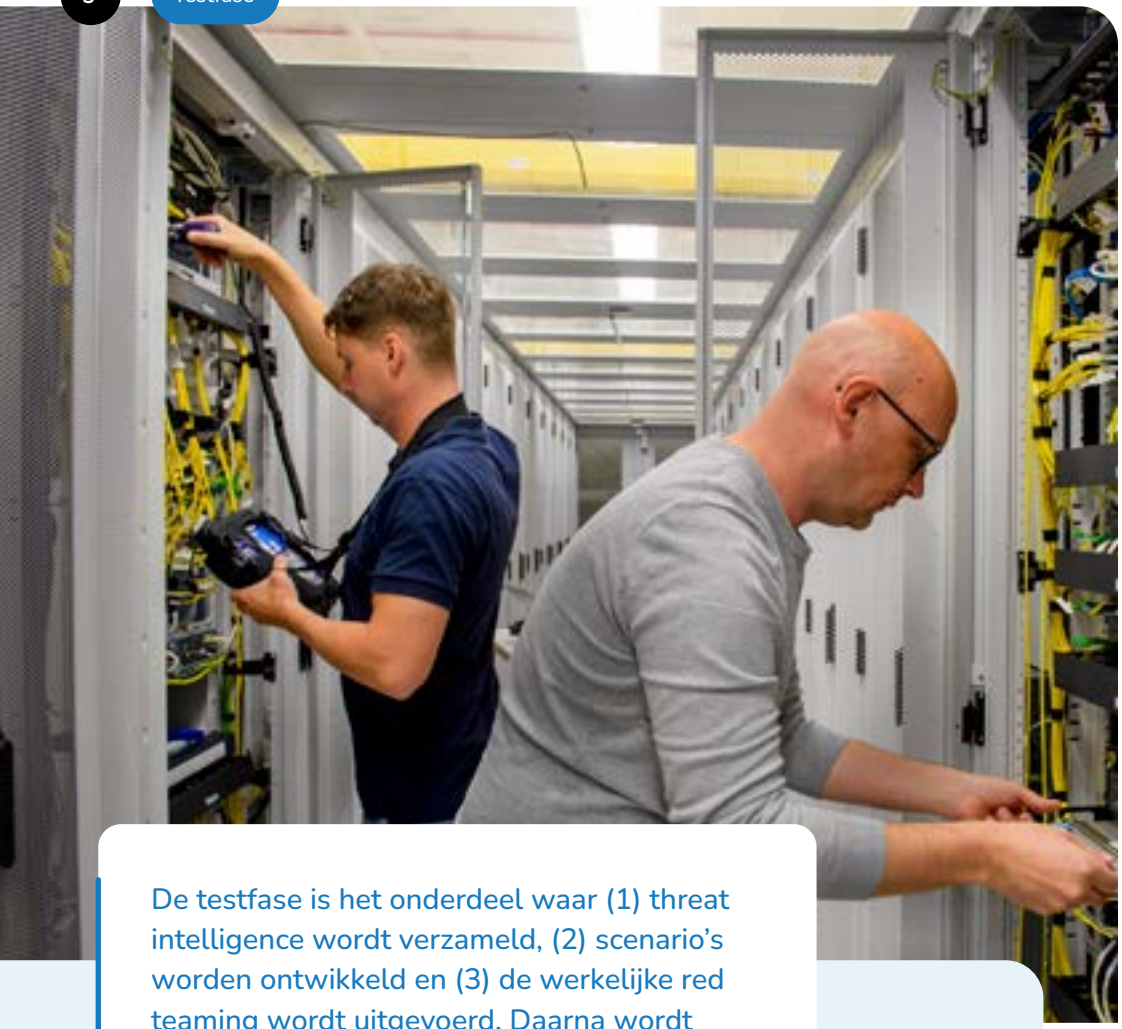
4.3 Inkoop

Op basis van de afgesproken scope en modules, start de Control Team Lead met de inkoop van een Red Team provider. De vlotte uitvoering van een ART-SURF-test vereist dat dit proces transparant is en dat de informatie en documentatie vrij kan stromen tussen de relevante partijen. Om de vrije informatiestroom te vergemakkelijken, kunnen geheimhoudingsovereenkomsten worden gebruikt. De offerteaanvraag die wordt gebruikt om een Red Team aan te besteden, wordt gedeeld met het SURF-TCT. Het inkoopproces start na de pre-launch bijeenkomst. Tijdens dit proces deelt de instelling een shortlist van mogelijke providers met het SURF-TCT. Het SURF-TCT kan contact leggen tussen de instelling en andere TIBER/ART/ART-SURF-instellingen om referenties op te vragen over de provider. Naast de verplichte bijeenkomsten moeten het SURF-TCT en het Control Team regelmatig bijeenkomen om de voortgang te bespreken. Het SURF-TCT kan, indien nodig, het Control Team ondersteunen in het inkoopproces of deelnemen aan workshops om een scopespecificatie op te stellen. Na de inkoop kan een launch bijeenkomst worden gehouden om alle belanghebbenden die aan de test deelnemen op elkaar af te stemmen. Tijdens deze bijeenkomst moeten afspraken worden gemaakt over de frequentie van de bijeenkomsten tijdens de TI- en Red Team-fasen, communicatiekanalen, documentatie en verantwoordelijkheden.

Bijeenkomsten
- Launch-bijeenkomst

Mijlpalen
- Succesvolle inkoopprocedure op basis van de testvereisten
- Ondertekende overeenkomst tussen de instelling en het Red Team

5 Voor kerntaken en activiteiten kan gebruikt worden gemaakt van de HORA en MORA businessmodel beschrijving



De testfase is het onderdeel waar (1) threat intelligence wordt verzameld, (2) scenario's worden ontwikkeld en (3) de werkelijke red teaming wordt uitgevoerd. Daarna wordt het blue team geïnformeerd en wordt de (4) Purple workshop uitgevoerd.

5 Test fase

5.1 Threat intelligence

De threat intelligence (TI) fase is de eerste actieve fase in een ART-SURF-test. Het omvat het verzamelen van informatie over de instelling en het identificeren van mogelijke dreigingen. Deze informatie wordt gebruikt om echte aanvalsscenario's te simuleren in de latere fasen van de test.

Eén van de eerste stappen in de TI-fase is een 'business overview workshop', georganiseerd door het Control Team. Het is van het grootste belang dat het Red Team en de TI-analist niet alleen de technische onderdelen van de instelling begrijpen, maar ook de bedrijfsprocessen. De business overview workshop, zal het Red Team en TI-Analist helpen om de scopespecificatie volledig te begrijpen en beter te beoordelen welke dreigingen van toepassing zijn op de instelling. Op basis van de scopespecificatie, de business overview workshop en eigen onderzoek, stelt de TI-analist een TI-rapport op met één of meer realistische dreigingsscenario's. De TI-analist kan hierbij ondersteund worden door een TI-specialist vanuit de instelling zolang dit de vertrouwelijkheid van de test niet schaadt. Dit is van meerwaarde omdat een interne TI-specialist veel kennis heeft van de systemen en dreigingen voor de instelling.

Op een nader bepaald tijdstip wordt een conceptversie van het TI-rapport geleverd. De TI-fase wordt afgesloten met een go/no go-bijeenkomst, bijgewoond door het SURF-TCT incl. TI-analist, het Red Team en het Control Team, alsook de sponsor op bestuursniveau. Tijdens de bijeenkomst presenteert de TI-analist zijn bevindingen en het bijbehorende TI-rapport. De sponsor op bestuursniveau keurt het/de gekozen scenario'(s) goed om het opstellen van een Red Team-plan door het Red Team te starten, op basis van het TI-rapport.

Bijeenkomsten

- Business overview workshop
- Go/no go-bijeenkomst TI-rapport

Mijlpalen

- Succesvolle ‘go-bijeenkomst’, die de start van de ART-SURF-test formaliseert
- Een ‘business overview workshop’ waarin de instelling informatie verstrekt over haar kritieke IT- en bedrijfsprocessen, doelstellingen en andere relevante ontwikkelingen aan de TI analist en het Red Team
- Succesvolle opzet (en goedkeuring) van het CT van één of meer op TI gebaseerde scenario’s die als basis dienen voor het Red Team-plan
- Oplevering van het threat Intelligence rapport vanuit SURF
- Een go/no go op het TI-rapport van SURF

5.2 Red teaming

De Red Team-fase bestaat uit een aantal stappen. Eerst worden het TI-rapport en de gekozen scenario’s omgezet in een aanvalsplan van het Red Team. Zodra dit plan is goedgekeurd door de sponsor op bestuursniveau, het SURF-TCT en Control Team, voert het Red Team het uit door de live systemen van de instelling aan te vallen. Het doel is om zwakke plekken, kwetsbaarheden en mogelijke hiaten in de verdediging van de instelling te identificeren, wat inzichten kan verschaffen die kunnen worden gebruikt om de cyberbeveiliging en paraatheid bij incidentrespons te verbeteren.

Het testplan van het Red Team

In het testplan zet het Red Team operationele aanvalsscenario’s uiteen voor de ART-SURF-test die:

- De door het Control Team en SURF-TCT goedgekeurde modules bevat;
- De TI-scenario’s gebruiken die zijn opgesteld in het TI-gedeelte van de ART-SURF-overeenkomst;
- Achtergrondinformatie voorzien over de handelswijze van het type dreigingsactor dat in de test wordt nagebootst;
- Bijkomende Open-source intelligence-informatie verzamelen die de gesimuleerde dreigingsactor helpt zijn doel te bereiken;
- TTP’s beschrijven die volgens het Red Team door de gekozen actor (zullen) worden gebruikt, op basis van zijn professionele kennis;
- In geval van een echte aanval, een impact zouden hebben op de kritieke functies van de instelling;
- Ook bepaalde elementen bevatten die de respons van de instelling testen en aantonen of de aanval onmiddellijk zou worden gedetecteerd of een redelijke kans zou hebben op succes.

De aanvalsscenario’s zijn geschreven vanuit het oogpunt van de dreigingsactor en zijn gebaseerd op threat intelligence. Het Red Team presenteert een aantal creatieve opties in elke testfase op basis van verschillende TTP’s die worden gebruikt door geavanceerde dreigingsactoren. Het doet dit om te anticiperen op veranderende omstandigheden of in het geval dat de eerste optie niet werkt. Het Red Team moet ook aangeven waar een leg-up nodig kan zijn als de aanval niet succesvol is en wat deze leg-up inhoudt. Het schrijven van het scenario is een creatief proces. De TTP’s bootsen deze na die in het verleden zijn waargenomen en kunnen technieken combineren die door verschillende relevante dreigingsactoren worden gebruikt om middelen te besparen. Het Red Team moet onderbouwen waarom het mogelijk is om meerdere technieken te combineren.

Rules of engagement

- Het testplan van het red team moet ‘rules of engagement’ bevatten, waarin het Red Team de regels vastlegt die het zal volgen. De rules of engagement moeten ten minste het volgende bevatten:
- Beschrijving op hoog niveau van de technieken die tijdens de aanval zijn gebruikt;
- Lijst van uitgesloten technieken;
- Gedetailleerde beschrijving van scenario’s die worden gebruikt voor social engineering;
- Hoe de privacy van zowel vrijwillige en onvrijwillige deelnemers wordt gewaarborgd in overeenstemming met relevante wetgeving.

Goedkeuring van het Red Team-plan

- Het testplan van het red team moet worden goedgekeurd:
- Vóór de start van de werkelijke testfase (door het Control Team en de Testmanagers);

Actieve red teaming

Nadat elke partij het aanvalsplan heeft goedgekeurd, start het Red Team met de actieve red teaming. Tijdens deze fase voert het een op intelligentie gebaseerde red teaming test uit op de doelsystemen. De scenario's zijn geen voorgeschreven draaiboeken die tijdens de test letterlijk moeten worden gevolgd. Als er zich obstakels voordoen moet het Red Team creatief zijn (zoals geavanceerde dreigingsactoren zouden doen) en alternatieve manieren ontwikkelen om het testdoel te bereiken. Dit gebeurt altijd in nauw overleg met het Control Team en de Testmanagers. Alle acties van het Red Team worden vastgelegd zodat ze kunnen worden herhaald met het Blue Team, als bewijs voor het Red Team-rapport en voor toekomstige referentie. De testdoelen zijn vooraf bepaalde 'vlaggen' die het Red Team tijdens de test moet proberen te bereiken terwijl deze de scenario's doorloopt; Het vastleggen gebeurt uiteraard in nauwe samenwerking met het Control Team en het algemene doel is om de capaciteiten van het Blue Team te verbeteren. Het scenario moet van begin tot einde worden uitgespeeld tenzij er voor de module 'Assumed Compromise' is gekozen.

Het Red Team kan wat hulp nodig hebben om barrières te overwinnen en kunnen ontdekt worden, maar het scenario moet volledig gebruik blijven maken van de ART-SURF-test binnen het gegeven tijdsbestek en alle fasen (in, door en uit) testen. Red Teams worden beperkt door de beschikbare tijd en middelen, alsook door morele, ethische en wettelijke grenzen. Het Red Team kan daarom af en toe leg-ups en/of informatie nodig hebben van het Control Team om voortgang te realiseren. Als dit gebeurt, moet de assistentie worden geregistreerd door het Red Team. Dit zorgt ervoor dat alle belanghebbenden maximaal voordeel halen uit de tijdsgebonden test.

Het Red Team staat te allen tijde in nauw contact met het Control Team en de Testmanagers. Het Control Team en de Testmanagers worden ten minste een keer per week door het Red Team bijgepraat over de voortgang. Fysieke bijeenkomsten tussen het Control Team, de Testmanagers en Red Team tijdens deze fase zijn sterk aangeraden, aangezien de besprekingen die hieruit voortkomen aanzienlijk bijdragen aan de kwaliteit van de test. In het geval van een in-through-out-scenario heeft de test een potentieel afkappunt. Als het Red Team de in-fase niet heeft kunnen voltooien, moet het realistische leg-ups krijgen zodat de rest van het scenario kan worden uitgespeeld. Als het Red Team voet aan grond heeft gekregen met een ander scenario, kan het toegestaan zijn om dat pad als alternatief te gebruiken voor de rest van het scenario waar de in-fase is mislukt.

Plan voor de Out-fase

Het aanvalsplan van het Red Team moet een uitgebreide beschrijving van de Out-fase bevatten. Het Red Team moet vóór de start van deze fase bepalen of de Out-fase zoals beschreven in het aanvalsplan van het Red Team nog steeds in lijn is met de huidige geplande uitvoering van het scenario. Zo niet, moet het Red Team aangeven hoe het de nieuwe Out-fase zal aanpakken. Dit moet niet worden vastgelegd in een formeel document, maar het Red Team moet aantonen dat hij de controle heeft over de Out-fase. Ongeacht of het in lijn is met de aanval, moet de Out-fase worden besproken met het Control Team en de Testmanagers vóór de uitvoering.

De Red Team-fase voltooien

De uitkomst van de Red Team fase is een testrapport, opgesteld door het Red Team en afgeleverd aan de instelling. Het conceptrapport moet binnen twee weken na de voltooiing van de test worden gedeeld. Het moet een overzicht geven van het hele ART-SURF-proces, inclusief de kritische functies, de scope, de threat intelligence basis van de test, de geplande scenario's, de uitgevoerde scenario's, de testbevindingen en het advies van het Red Team aan de instelling. Op dit punt worden de belangrijkste leden van het Blue Team van de instelling op de hoogte gebracht van de test. Op basis van het conceptrapport kunnen ze hun eigen tijdlijn samenstellen van de aanval vóór de Purple workshop.

Bijeenkomsten

- Go/no go-bijeenkomst voor het testplan van het Red Team
- Go/no go-bijeenkomst voor het uit-plan
- Wekelijkse updates

Mijlpalen
- Definitieve versie van het Red Team-testplan
- Oplevering van het Red Team-plan
- Een go/no go op het Red Team-plan
- Behalen van gestelde vlaggen tijdens de Red Teaming-fase
- Oplevering Red Team-rapport
- Oplevering Blue team tijdlijn en acties

5.3 Purple workshop

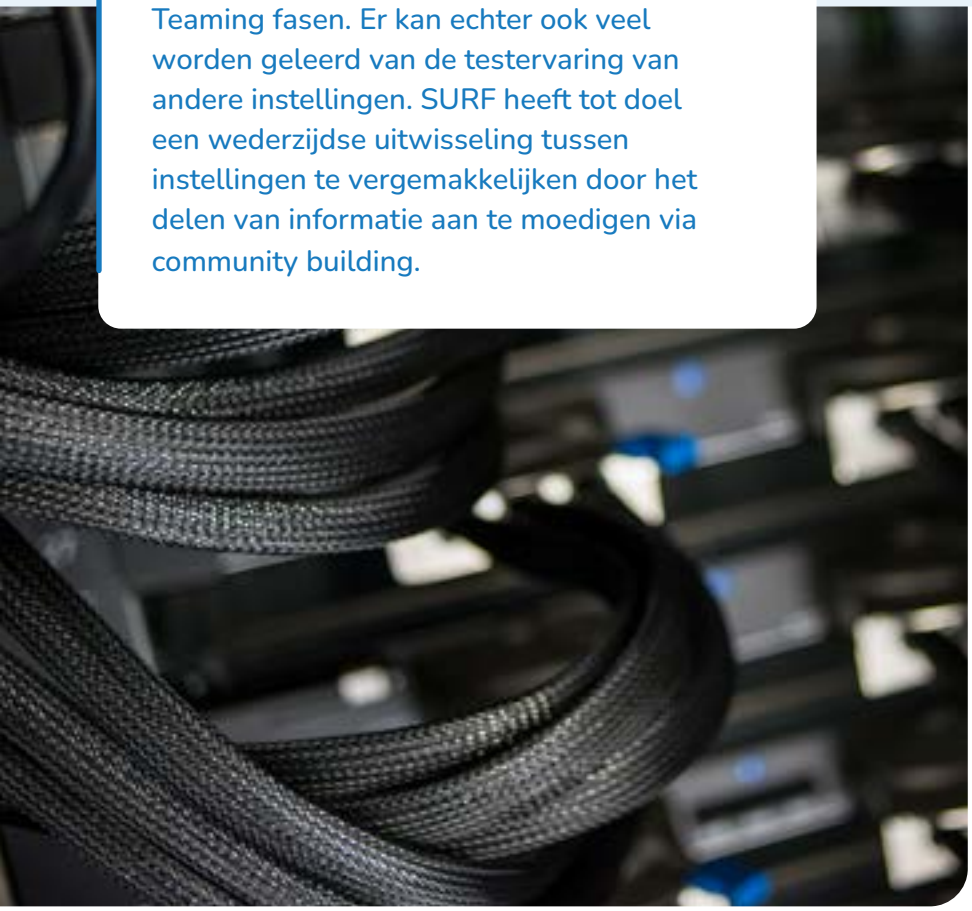
De instelling organiseert een Purple workshop nadat het Red Team zijn conceptrapport heeft afgeleverd. Vaak wordt de Purple teaming-fase ervaren als de meest leerzame fase, waardoor deelnemers meer tijd besteden aan dit deel van het proces. De doelstelling van deze workshop is om de leerervaring te vergroten. Het is geen losse Purple teaming test, maar een workshop op basis van de geleerde lessen uit de red teaming fase. Deze workshop kan één dag (Purple Teaming-basis) of twee dagen (Purple Teaming-uitgebreid) duren, afhankelijk van de scope en duur van de test.
De Purple workshop in ART-SURF vergroot de leerervaring voor zowel het Blue Team als het Red Team. Tijdens de Purple workshop spelen het Red Team en de instelling de aanval opnieuw af en werken zij samen om de verdediging van de instelling te verbeteren op basis van de lessen uit de test. De Testmanagers zijn hierbij graag aanwezig om de test in context te plaatsen en lessen mee te nemen voor de bredere sector. De Purple workshop hoeft niet altijd volledig technisch te zijn en kan, afhankelijk van het gespeelde aanvalsscenario, soms meer procesgericht zijn. Dan is het handig om ook niet securityspecialisten te betrekken.

Bijeenkomsten
- Purple Teaming-planningssessie

Mijlpalen
- Uitvoering van de Purple workshop met het Blue en Red Team
- Oplevering definitieve versie van het Red Team-rapport

6 Afsluitingsfase

De instelling leert veel over haar eigen niveau van cyberweerbaarheid tijdens de threat intelligence, red teaming en Purple Teaming fasen. Er kan echter ook veel worden geleerd van de testervaring van andere instellingen. SURF heeft tot doel een wederzijdse uitwisseling tussen instellingen te vergemakkelijken door het delen van informatie aan te moedigen via community building.



6.1 Feedbacksessie

Tijdens de feedbacksessie komen het Control Team, SURF-TCT en het Red Team samen om de ART-SURF test te evalueren. De Testmanagers organiseren en faciliteren de workshop. Het doel is om de leerervaring van alle betrokkenen bij het proces verder te faciliteren en toekomstige testen te verbeteren. Het is niet de bedoeling om de test resultaten te evalueren.

6.2 Mitigatieplan

De instelling stelt een mitigatieplan op, op basis van de testresultaten. De ART-SURF-documentatie kan worden gebruikt ter ondersteuning van de business case voor de implementatie van verbeteringen om de tijdens de ART-SURF-test geïdentificeerde kwetsbaarheden te verminderen. De TI- en Red Team rapporten kunnen dienen als input voor het mitigatieplan. Verdere input kan komen van het Control Team en organisatorische bevindingen. Het SURF-TCT is niet betrokken bij de opstelling van het mitigatieplan.

6.3 Rapporteren op bestuursniveau

Het is van het grootste belang dat het bestuur van de instelling op de hoogte is van de dreigingen, testresultaten en het mitigatieplan. Daarom is het bespreken van de test tijdens een bestuursvergadering onderdeel van de afsluitingsfase. Indien gewenst door de Control Team Lead woont het SURF-TCT de presentatie van de resultaten en bevindingen aan het bestuur bij. Het SURF-TCT moet dan het belang benadrukken van de betrokkenheid, steun en verantwoordelijkheid van het bestuur bij de uitvoering van het mitigatieplan.

6.4 De lessen delen

Het idee achter het ART-SURF programma is dat alle instellingen die meedoen met het programma kunnen leren van alle testen die gedaan worden in plaats van alleen van hun eigen test. Dit zorgt voor een sector die weerbaarder wordt en testen zijn hierdoor meer kosteneffectief. Om dit te bewerkstelligen is het wel nodig dat alle deelnemers van het ART-SURF programma hun lessen delen.

Het (mondeling) delen van de geleerde lessen is een verplicht onderdeel van ART-SURF en noodzakelijk voor het verkrijgen van het ART-SURF label. Het delen zal door SURF gefaciliteerd worden in SCIRT-sessies en sectorale CISO-bijeenkomsten onder TLP: ROOD[6]. Dit betekent dat deze informatie niet met mensen buiten de groep gedeeld mag worden. Instellingen kunnen hierbij zelf besluiten hoeveel informatie precies wordt gedeeld op basis van het gremia en in hoeverre de bevindingen al zijn opgelost.

Het is van belang dat geleerde lessen zo snel mogelijk worden gedeeld zoals bij de eerste of opvolgende SCIRT/CISO bijeenkomst na afronding van de ART-SURF test. De verwachting is in ieder geval dat een instelling 3 maanden na afronding van de test haar resultaten binnen de sector heeft gedeeld. Daarnaast kan SURF vanuit haar SURF-TCT-rol op niet-herleidbare basis lessen uit de verschillende testen gebruiken om haar producten te verbeteren of instellingen te informeren om de cyber weerbaarheid te verhogen. Dit zal altijd gebeuren in overleg en afstemming met de instelling.

6.5 De test voltooien

Na het voltooien van de test, het delen van de resultaten en het voltooien van de Purple Teaming, moet de Control Team Lead ervoor zorgen dat alle sporen van de test worden verwijderd. Dit betekent dat eventuele sporen van malware die tijdens de test zijn gebruikt, moeten worden verwijderd en dat de deelnemende teams alle testgegevens verwijderen. Het Red Team moet de Control Team Lead bijstaan en alle communicatiegroepen moeten worden ontbonden (tenzij ze nog steeds nodig zijn). Hierna gaan de Control Team Lead en het SURF-TCT akkoord dat de ART-SURF-test beëindigd is.

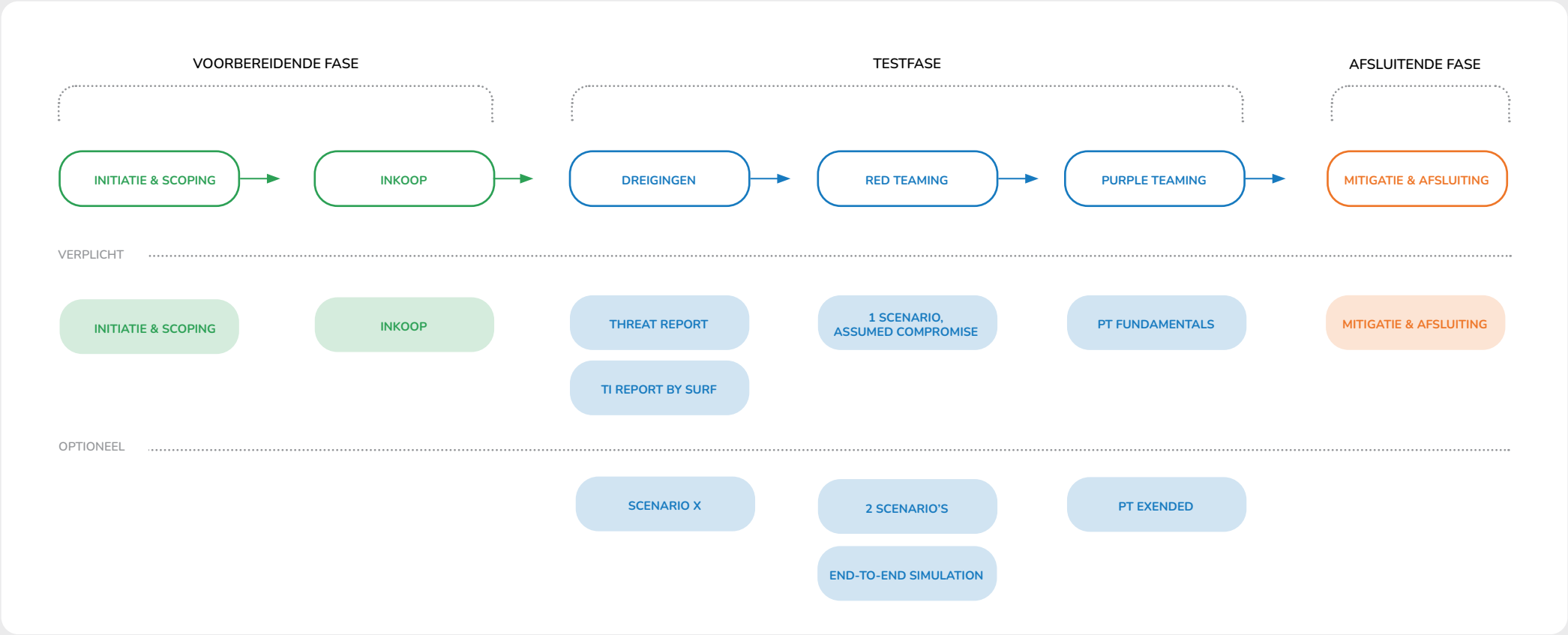
Traffic Light Protocol zie https://www.ncsc.nl/aansluiten-en-samenwerken/traffic-light-protocol-tlp

Bijlage 1: Afkortingen

ART	Advanced Red Teaming
DNB	De Nederlandsche Bank
IT	Informatietechnologie
SOC	Security Operations Center
TCT	Test Cyber Team
TI	Threat intelligence
TIBER	Threat intelligence-based ethical red teaming
TLP	Traffic Light Protocol
TTP	Tactiek, Technieken en Procedures gebruikt in een cyberaanval

Bijlage 2: Testoverzicht

Deze bijlage geeft een volledig overzicht van het ART-SURF proces en de verschillende verplichte en optionele modules.



Bijlage 3: Wijzigingen tussen ART en ART-SURF

ART-SURF is de implementatie van het ART-raamwerk zoals dat ook in andere sectoren wordt gebruikt, met uitzondering van een paar punten. Deze verschillen moesten worden aangepast om aan te sluiten bij de behoeften van de onderwijs- en onderzoeksector. Deze bijlage geeft een overzicht van fundamentele wijzigingen zodat providers vlot kunnen beoordelen waarin ART-SURF verschilt van andere ART-raamwerken.

Algemeen

- Het Test Cyber Team wordt SURF-Test Cyber Team genoemd (SURF-TCT)
- Kritische functies worden binnen ART-SURF is gedefinieerd als: *"Kerntaken of activiteiten van een instelling die wanneer verstoord in termen van beschikbaarheid, integriteit of vertrouwelijkheid een serieuze impact hebben op de doelen van de instelling, de bredere sector of de Nederlandse samenleving."*

Threat Intelligence

- Threat Intelligence is verplicht, maar wordt geregeld door SURF in plaats van een commerciële Threat Intelligence provider. Een TI-analist van SURF stelt een Targeted Threat Intelligence rapport op voor de instelling, naast een dreigingsrapport dat aan alle SURF-leden wordt geleverd. Daarom zijn alle andere threat intelligence modules verwijderd.

Red Teaming

- Het Blue Team ontvangt een conceptversie van het Red Team-rapport om hun eigen tijdlijn te maken.

Gold Teaming

- Gold teaming is verwijderd. Instellingen kunnen het Red Team-scenario natuurlijk wel gebruiken als input voor eigen oefeningen en in samenwerking met SURF zoals NOZON.

Afsluitingsfase

- Het adresseren van de test bij een bestuursvergadering is verplicht met aanwezigheid van het Red Team.
- De test samenvatting is verwijderd en vervangen door verplichte mondelinge besprekingen van de testresultaten in SURF-gremia.
- De 360 feedbacksessie is hernoemd naar feedbacksessie.
- Een feedbackrapport is niet vereist, de feedback kan worden besproken tijdens de bijeenkomst zonder verplichte documentatie
- Het is aan de instelling om de resultaten te delen met haar toezichthouder
- Een attest is geen is geen standaard onderdeel van het proces

colofon

Auteurs
Maarten Bras
Joost Gadellaa
Charlie van Genuchten
Abdul Altawekji

Vormgeving
Vrije Stijl BNO, Utrecht

Juni 2025


SURF