Red Teaming in de praktijk – Scoping, opdrachtbepaling en inkooprichtlijn

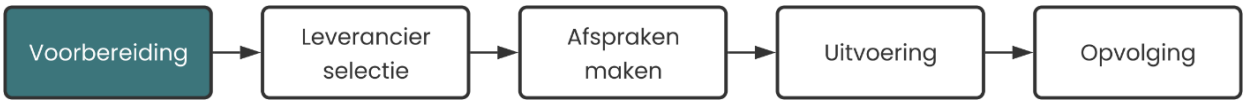
SURF

Auteur(s): CIP, aangepast door SURF: Charlie van Genuchten
Versie: 1.0
Datum: 1 december 2023

Deze publicatie is afgeleid van het Whitepaper *Red Teaming in de praktijk* van het CIP: https://www.digitaleoverheid.nl/document/red-teaming-in-de-praktijk/

Inhoudsopgave

1 Voorbereiding – scope



Een aanvalssimulatie is geen kwestie van even een red team inhuren en hun gang laten gaan. Om er het maximale uit te halen moet de organisatie van tevoren zijn huiswerk doen. Dat levert een betere vraagstelling op bij de aanbieder en meer controle over het proces. Je wilt niet overgeleverd zijn aan de grillen van een leverancier. De goede leveranciers zullen je bij de intake ook vragen naar de onderstaande zaken.

1.1 Definieer het doel van de red team oefening

Wat is het gewenste eindresultaat van de red team oefening?
Waar wil ik de red team oefening voor gebruiken, wanneer is het een succes?

De scope en vorm van een red team oefening zal afhangen van het uiteindelijke doel. Die doelen kunnen heel gevarieerd zijn, maar moeten wel helder zijn vóór je een red team oefening aanvraagt. Mogelijke doelen zijn:

- Gaten in jouw monitoring en detectie opsporen;
- Jouw monitoring en detectie verbeteren;
- De effectiviteit van jouw SOC onderzoeken;
- Onbekende risico's identificeren (aanvallers denken immers anders);
- Awareness creëren binnen de organisatie of bij de directie;
- Aantonen dat jouw organisatie in control is;
- Het management overtuigen dat er meer bewustzijn en budget nodig is voor security;
- Jouw blind spots identificeren.

Bedenk dat een red team oefening voor veel van de doelen hierboven een hulpmiddel is, geen wonderpil. Vaak zul je ook andere instrumenten in moeten zetten om zo'n doel volledig te halen.

1.2 Dreigingsbeeld vaststellen

Waar moet ik bang voor zijn?

Verschillende managementtrainingen maken gebruik van een rollenspel, waarbij een acteur die ene collega naspeelt die het bloed onder je nagels vandaan haalt. Door het naspelen van een zo reëel mogelijke situatie leren we hoe we het beste kunnen reageren. Zo'n rollenspel werkt alleen als we de acteur van tevoren inlichten over de situatie en het gedrag van de betreffende collega. Hoe meer informatie we verschaffen, hoe reëler de acteur de situatie kan neerzetten en hoe groter het leereffect.

Het red team is de acteur in deze aanvalssimulatie. Ook hier geldt dat meer startinformatie zorgt voor een betere oefening. Wat zijn de reële dreigingen? Waar liggen mijn zwaktes? Wie moet het red team spelen? Een ransomware-crimineel die het netwerk wil platleggen? Een statelijke actor die op bepaalde informatie uit is? Een red team leverancier kan veelal via verschillende scenario's werken. Door een aanvalsscenario te kiezen dat ook relevant is voor

je instelling, vergroot je het effect van de opdracht. Hierbij kan een leverancier bijvoorbeeld rekening houden met technieken die vaak gebruikt worden door bepaalde actoren.

Het helpt om vooraf **samen met het red team** tot een zo nauwkeurig mogelijk dreigingsbeeld te komen. Je kunt dit zelf opstellen, maar je kunt het ook laten doen door de red team provider, of zelfs door een derde partij. Maak hier bijvoorbeeld ook gebruik van het cyberdreigingsbeeld dat SURF voor de sector publiceert. Via het Security Expertise Centrum (SEC) kan SURF ook verder ondersteunen.

Het vooraf verschaffen van deze informatie lijkt misschien op valsspelen maar is integendeel juist een hulpmiddel waardoor het red team de simulatie beter kan uitvoeren. Een red team oefening is geen wedstrijd tussen rood en blauw, maar een manier om met de beschikbare tijd en middelen een optimaal resultaat te halen. De keuzes die je maakt hebben invloed op de test en het budget.

1.3 Aanvalsvormen uitsluiten

Welke aanvalsvormen wil ik uitsluiten?
Een van de keuzes die je maakt, is of fysieke aanvalsvectoren wel of niet meegenomen moeten worden. Fysieke aanvallen komen voor (een Wi-Fi-antenne op de parkeerplaats, een Raspberry Pi in het netwerk inpluggen) maar zijn zeldzaam en vaak gebonden aan een bepaald soort actoren. Wellicht kunnen ze in jouw scenario uitgesloten worden. Dit hangt sterk samen met je doel. Social engineering en phishing kunnen veel toevoegen voor awareness omdat ze erg tot de verbeelding spreken. Ze kosten echter veel tijd en dus geld. Wil je zo veel mogelijk technische bevindingen? Dan ligt assumed compromise meer voor de hand.

Als **social engineering** niet uitgesloten wordt, dan zal de leverancier daadwerkelijk proberen om fysiek binnen te komen op een van je locaties en van daaruit proberen om ook in je digitale systemen binnen te komen. Veelal heeft onze sector een open karakter, waardoor het moeilijker is om je tegen indringers te verdedigen die bewust bij je naar binnen willen. Wel is de vraag hoe ver ze kunnen komen én of je monitoring en detectie het (tijdig) doorheeft.

Een andere vorm van social engineering is het uitvoeren van een **phishing campagne**. Als dit ingezet wordt, dan zal de leverancier proberen om ergens credentials te krijgen (loginnaam/wachtwoord). En dus ook medewerkers en/of studenten benaderen, bijvoorbeeld met phishing mails. Mocht dit geen onderdeel zijn van de scope, dan dient de leverancier zelf te kijken of hij via (technische) zwakheden in de infrastructuur aan credentials kan komen.

Een derde alternatief betreft de **assumed compromise**: hierbij gaan we ervanuit dat de hacker de beschikking heeft over een studenten- en/of medewerkers account. Dat biedt dan de basis voor de leverancier om te kijken of hij deze credentials kan verhogen. Door uit te gaan van een assumed compromise, kan mogelijk een hoop tijd (en dus budget) bespaard worden die een leverancier anders besteed aan het zelf zoeken naar een eerste set basis credentials.

In elk geval is het verstandig om afspraken met de leverancier te maken over hoe lang er wordt gephished e.d., om vervolgens over te gaan op een assumed compromise om tijd te besparen. Over dit soort manieren van inkorten lees je meer in paragraaf 3.5.

1.4 De kroonjuwelen van jouw organisatie

Wat zijn de kroonjuwelen van mijn organisatie?

Deze zal je koste wat het kost willen beschermen. Ze zijn het doelwit van hackers, en daarmee ook van het red team. Wat zijn de meest essentiële assets van de organisatie? Waar ligt het bestuur bij wijze van spreken 's nachts van wakker? Vraag it ook expliciet uit bij bestuurders, daarmee vergroot je de betrokkenheid en verrijk je de analyse.

Denk daarbij niet alleen aan techniek. Een incident waarbij een aanvaller domain administrator weet te worden, is op zichzelf nog geen ramp. Het kwijtraken van de controle op systemen of de manipulatie van examenresultaten zijn dat wellicht wel. Dit is binnen jouw organisatie als onderdeel van een risicoanalyse wellicht al eens in kaart gebracht. Hierbij kan je ook gebruik maken van de toolkit risicobeoordeling.

Zodra je de kroonjuwelen hebt bepaald kun je dit meegeven aan de leverancier, zodat die gericht kan kijken of een inbreuk op die kroonjuwelen mogelijk is of niet. Daarbij is het de keuze hoeveel informatie je de leverancier meegeeft ten aanzien van de infrastructuur van je instelling. Moet hij zelf zien uit te zoeken in welk netwerksegment hij moet zoeken? Of geef je dat vooraf al mee? In de regel geldt dat hoe meer je meegeeft, hoe minder tijd een leverancier nodig zal hebben, en hoe goedkoper de uitvoering van de opdracht is.

Overigens, kijk ook naar de maatregelen die je zelf hebt genomen om de kroonjuwelen te beschermen. De red team oefening is namelijk bedoeld om die maatregelen te testen. Dat betekent ook dat een red team oefening zinloos is als er nog geen of onvoldoende maatregelen genomen zijn. Een zekere mate van volwassenheid in het beveiligingsdomein is noodzakelijk. Is die er niet, dan zijn er waarschijnlijk betere manieren om het beveiligingsniveau te verhogen alvorens aan een red team oefening te beginnen (zie de keuzekaart securitytesten op het SEC).

1.5 Gewenste rapportage en terugkoppeling

Het is belangrijk om vooraf goed te bepalen op welke niveaus je terugkoppeling wilt hebben van de leverancier. Veelal worden de volgende drie vormen gekozen:

1. Rapportage op management niveau: deze kan gebruikt worden om binnen de organisatie ook het hogere management mee te nemen in de uitkomsten en resultaten van de test. Dit bevat ook op hoofdlijnen de maatregelen die aangeraden worden om geconstateerde kwetsbaarheden te verhelpen;
2. Rapportage op detailniveau: hierin staat in detail hoe de aanval is uitgevoerd, welke tijdlijnen er zijn geweest en welke detectie heeft plaatsgevonden. Deze rapportage is bedoeld voor het blue team om daadwerkelijke verbeteringen door te kunnen voeren, bijvoorbeeld door direct poorten dicht te zetten en/of configuraties aan te passen;
3. Bespreking van de rapportage op detailniveau door red team en blue team samen. Neem de tijd voor deze bespreking, hier wordt het meest geleerd!

1.6 Budget

Wat is mijn budget?

Stel een realistisch budget vast in overeenstemming met jouw wensen. Kies met een beperkt budget voor een beperkte scope.

Hoewel verschillende aanbieders verschillende prijzen zullen hanteren, willen we toch een zeer ruwe indicatie geven van de kosten die verbonden zijn aan een red team oefening. We doen dat in de vorm van de tijd die de verschillende onderdelen van een red team oefening kosten. De werkelijke tijdsduur kan afwijken van de indicatieve duur – dit hangt onder meer af van de gekozen scenario's en einddoelen.

Fase	**Tijdbesteding**
Voorbereiding / rules of engagement opstellen	1 dag - 1 week
Threat intelligence	1 week - 4 weken
Red team oefening IN fase	2 weken - 8 weken
Red team oefening THROUGH fase	2 weken - 8 weken
Red team oefening OUT fase	1 week - 4 weken
Rapportage	1 week - 2 weken
Purple teaming sessie (achteraf)	1 dag - 2 weken

Het is lastig om goede indicatie te geven hoe duur een red team opdracht daadwerkelijk gaat worden. Dat hangt echt af van de scope, en deels ook van de leverancier die gekozen wordt. Bovenstaande tabel geeft een indicatie, hoe meer tijd besteed wordt, hoe hoger de kosten zullen zijn. Keuzes in scope zijn dan ook nodig als het budget beperkt is. De goedkoopste test die SURF kent was rond de 30.000 euro. Veelal is het dubbele nodig, ook soms meer dan dat. Neem contact op met het SEC om te kijken of we een indicatie kunnen geven van de kosten waar je rekening mee moet houden op basis van jouw scope.

1.7 Planning en looptijd

Wanneer moet de oefening plaatsvinden? Hoe lang kan de oefening ongeveer duren? Wanneer mag niet geoefend worden?

Een red team oefening vraagt tijd en capaciteit van de organisatie. Daar moet met de planning rekening mee worden gehouden om de organisatie niet op de verkeerde momenten te veel te belasten. Ook moet vastgesteld worden wanneer het red team **niet** mag aanvallen. Hoewel daarmee enigszins in realisme wordt ingeboet kan het toch verstandig zijn om ze tijdens het weekend, de zomervakantie of tijdens deelname aan (N)OZON, even te laten stoppen.

Ook over de doorlooptijd moet nagedacht worden. Een langere doorlooptijd geeft het red team de gelegenheid om de activiteiten meer te spreiden. Het security team heeft meer gelegenheid om de activiteiten van het red team te detecteren. Aan de andere kant geeft dit

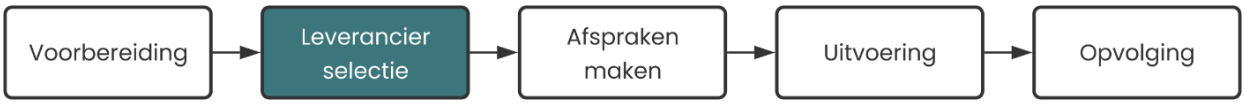
het red team de mogelijkheid om door de spreiding van activiteiten minder op te vallen. Afhankelijk van het gekozen scenario kan dit een betere benadering van de werkelijkheid zijn.

1.8 Checklist voorbereiding – scope

Voor je begint aan een red team oefening dien je op de volgende vragen antwoord te kunnen geven.

- ☐ Wat is het doel van de oefening?
- ☐ Wat is het dreigingsbeeld voor mijn instelling?
- ☐ Wat zijn goede potentiële aanvalsscenario's?
- ☐ Welke vorm van red team oefening sluit het beste aan bij mijn doel?
- ☐ Welke aanvalsvormen wil ik uitsluiten?
- ☐ Wat zijn de kroonjuwelen van mijn organisatie?
- ☐ Welke maatregelen heb ik genomen om ze te beschermen?
- ☐ Wat is mijn gewenste eindresultaat van de red team oefening?
- ☐ Wat is mijn budget?
- ☐ Wanneer mag de oefening starten, hoelang mag ze duren, wanneer mag niet geoefend worden?

2 Leverancier selectie



Voor het uitvoeren van een red team moet een leverancier geselecteerd worden. Check hiervoor het inkoopbeleid van je instellingen: afhankelijk van hoe groot of klein de opdracht is, kan je mogelijk een onderhandse uitvraag doen, of moet je een openbare aanbesteding houden.

Bij een aanbestedingsprocedure is het van belang een heldere uitvraag te doen. Hoe beter je weet wat je wilt, des te specifieker is je offerteaanvraag en des te beter kun je offertes tegen elkaar afwegen. In het voorgaande hoofdstuk beschreven we wat je zelf moet voorbereiden, hier wat je kunt vragen van de leverancier.

2.1 De offerte aanvraag

Voor je een offerte aanvraagt zul je het voorwerk uit hoofdstuk 1 grotendeels afgerond moeten hebben. Aanbieders kunnen een betere offerte uitbrengen als de volgende zaken in *generieke* termen al in de uitvraag zijn vermeld:

- Wat is het doel van de red team oefening?
- Waar ben ik bang voor?
- Wat zijn de kroonjuwelen van mijn organisatie? [NB dit kan je ook in een later stadium bespreken]
- Wat is mijn budget?
- Welke maatregelen wil ik testen?
- Welke vorm moet de red team oefening hebben?
- Hoe uitgebreid wil ik testen?
- Zit social engineering ook in scope?
- Wie levert de dreigingsinformatie en hoe specifiek moet deze zijn?
- Wat zijn de gewenste eindproducten (rapportage, bijeenkomst, zie ook 2.5)?

Het antwoord op een aantal van deze vragen wil je misschien niet zomaar delen. In dat geval kun je de aanbieders om een geheimhoudingsverklaring vragen.

Aanbieders begrijpen dat het bovenstaande wensenoverzicht indicatief is en er in overleg verfijningen en aanpassingen kunnen worden aangebracht. Om misverstanden te voorkomen is het wel aan te raden om de uiteindelijke afspraken met de aanbieder op papier vast te leggen. Stem dit proces sowieso goed af met je inkoopafdeling om te voorkomen dat de opdracht onrechtmatig wordt verleend.

Vanuit SURF kijken we graag mee met opdrachten die uitgevoerd wordt. Hierdoor krijgt SURF ook steeds meer zicht op wat verschillende leveranciers bieden. Neem contact op met het SEC om te kijken of we je kunnen helpen bij de preselectie van leveranciers en hoe we hier goede afspraken over kunnen maken.

2.2 Vragen aan de aanbieder(s)

Niet alleen jij moet je huiswerk doen, ook de aanbieder moet kunnen aantonen dat hij zijn huiswerk gedaan heeft. Hieronder een aantal vragen die je aanbieders kunt stellen om de serieuze aanbieders van de cowboys te onderscheiden. De antwoorden op deze vragen kunnen vooraf gegeven worden, maar zouden ook terug te vinden moeten zijn in de offerte.

- **Generiek dreigingsbeeld:** Een serieuze aanbieder moet direct kunnen vertellen wat het huidige dreigingslandschap is, en voor welke actoren en aanvalsmethodieken het meest gevreesd moet worden. Ze zullen over het algemeen geen dreigingsbeeld klaar hebben liggen voor jouw specifieke branche en locatie, aangezien dit maatwerk is.

- **Voorbeeldrapportage:** Dat geeft inzicht in wat en hoe uitgebreid er gerapporteerd wordt en hoe dat aansluit bij jouw wensen. De aanbieder zal in de voorbeeldrapportage allicht bepaalde delen hebben verwijderd om de privacy van een eerdere klant te beschermen. Een rapportage dient voldoende informatie te bevatten voor het blue team om de aanvalsstappen terug te zoeken in hun systeem. De rapportage moet niet alleen bevatten wat het red team gedaan heeft, maar ook wanneer. Een rapportage hoeft geen document te zijn, maar kan ook in de vorm van een presentatie gegeven worden. In dat geval kan de aanbieder als voorbeeld een slidedeck van zo'n presentatie kunnen laten zien.

- **Framework:** Gebruikt de aanbieder een formeel kader of werkt hij volgens 'een eigen' model of zonder kader?

- **Scenario's:** Een realistisch aanvalsscenario bouw je over het algemeen niet alleen. Als je gaat voor een generiek scenario, dan zal de aanbieder deze als het goed is al hebben klaarliggen. Voor een meer specifiek scenario is samenwerking tussen opdrachtgever een aanbieder nodig. Beiden bezitten relevante kennis die de ander niet heeft.

- **Competentie:** Een goede aanbieder zal graag zijn competentie aantonen. Je wilt de volgende zaken weten van een potentiële aanbieder: Certificering, opleidingen, publicaties

- **Referenties:** Vraag of de aanbieder je in contact kan brengen met voorgaande klanten, bij voorkeur in dezelfde sector. Van hen kun je meer horen over de aanpak van de aanbieder.

- **Screening**: Als geheimhouding noodzakelijk is heb je mogelijk als extra eis dat de medewerkers van de aanbieder een veiligheidsonderzoek hebben gehad of Verklaring Omtrent het Gedrag (VOG) kunnen tonen.

2.3 Offertes beoordelen

Een offerte dient antwoord te geven op de geformuleerde vragen en wensen. Let daarnaast op de volgende criteria:

- **Aanpak en planning**: Hoeveel tijd denkt de aanbieder nodig te hebben? Is dit helder beargumenteerd? Is duidelijk omschreven hoe men gaat testen? Zijn de verschillende fases van de test beschreven?

- **Omgang met gevoelige informatie:** Meldt de offerte hoe de aanbieder omgaat met gevoelige informatie? Wordt melding gemaakt van een geheimhoudingsverklaring, verwerkersovereenkomst en bewaartermijn? De offerte hoeft dit niet uit te spellen. Je kunt hierover ook in een latere fase afspraken maken met de door jou gekozen aanbieder.
- **Prijs:** Je moet de prijs afwegen tegen de kwaliteit van het aanbod. Als het doel is om het securityteam te trainen en een laaggeprijsd aanbod gebruikt geen formeel model en rept niet over een rapportage of evaluatie, dan voldoet dit aanbod niet aan je eisen.

- **Scenario's:** De gebruikte scenario's zullen niet uitgeschreven staan in de offerte, maar het aantal scenario's en de diepte ervan wel. Realistische scenario's horen bij de prijs inbegrepen te zijn.

- **Kwaliteit van de offerte:** Adresseert de offerte alle bovengenoemde punten in een overzichtelijk geheel of heeft de aanbieder deze gegevens buiten de offerte om verstrekt?

2.4 Checklist Leverancier Selectie

Let bij het kiezen van een geschikte leverancier op de volgende zaken:

- ☐ Vraag de aanbieder naar het huidige dreigingsbeeld;
- ☐ Vraag de aanbieder om een voorbeeldrapportage;
- ☐ Vraag de aanbieder welk kader hij gebruikt om de scenario's aan op te hangen;
- ☐ Vraag de aanbieder hoe zij voor realistische scenario's zorgen, of hoe ze daarbij helpen;
- ☐ Vraag de aanbieder naar een generiek scenario;
- ☐ Vraag de aanbieder zijn competentie aan te tonen;
- ☐ Heeft de aanbieder de test en de tijdsduur helder en onderbouwd omschreven?
- ☐ Zijn er afspraken te maken over het omgaan met gevoelige informatie?
- ☐ Zijn prijs en kwaliteit in balans?
- ☐ Nodig de aanbieder uit zijn offerte toe te lichten en vragen te beantwoorden.

3 Afspraken maken

Je hebt jouw huiswerk gedaan en uit de aanbieders een leverancier geselecteerd, wat nu? Voor de uitvoering van de red team oefening gaat beginnen zullen nog een aantal afspraken met de leverancier moeten worden gemaakt.

3.1 Wanneer uitvoeren?

Spreek met de leverancier een startdatum en doorlooptijd af. De oefening drukt ook op jouw resources en kan daarmee business impact hebben – wanneer past het in de planning? In het onderwijs is het gangbaar om de start van de inschrijvingen, de start van het onderwijs na de zomer, en de tentamenperiodes uit te sluiten. Zeker voor het laatste kan het voldoende zijn om af te spreken dat er één of twee weken pauze wordt gehouden, wat het realisme juist ten goede komt. Andersom wil je met een red team de realiteit zo goed mogelijk simuleren en daarom misschien niet het 'rustigste' moment kiezen.

3.2 Juridisch kader

Het is sterk aan te raden om voorafgaand aan de red team oefening juridische afspraken te maken. Beide partijen nemen risico's die afgedekt moeten worden. In de meeste gevallen is een standaard overeenkomst voldoende, maar ook hier is soms maatwerk noodzakelijk. Elementen van het juridisch kader (denk aan de vrijwaringsverklaring) kunnen ook al in de offerte worden opgenomen.

Een juridisch kader zal onder meer de volgende elementen omvatten:

- **Scope**: Wat wordt wel en wat wordt niet getest? Denk hierbij aan uw IT-leveranciers, IP-ranges, uw procesautomatisering, etc.
  Uitsluitingen worden bij voorkeur expliciet opgenomen;
- **Vrijwaring**: Het uitvoeren van een red team oefening is zonder toestemming van de opdrachtgever strafbaar. Beide partijen gaan een overeenkomst aan waarbij het red team gevrijwaard wordt van vervolging. Je geeft het red team toestemming om in te breken op en te bewegen binnen de systemen. Waar van toepassing moeten de IT-leveranciers ook toestemming geven;
- **Aansprakelijkheid**: De opdrachtgever mag ervan uitgaan dat de leverancier de opdracht op een verantwoordelijke en zorgvuldige wijze uitvoert. Als de leverancier bewust of onbewust buiten de afspraken om schade aanricht dan zal zij hier echter in de regel zelf voor aansprakelijk zijn. Afspraken over aansprakelijkheid dienen vooraf vastgelegd te zijn.
- **Verwerkersovereenkomst**: In sommige scenario's verwerkt het red team persoonsgegevens en zal zich daarbij aan de AVG moeten houden. Ook over de opslag en verwerking van andere gegevens dienen afspraken te worden gemaakt;
- **Geheimhoudingsverklaring**: gevoelige informatie die door jou verstrekt of tijdens de oefening gevonden wordt, mag niet gedeeld worden met derden;
- **Bewaartermijnen**: Binnen welke termijn wordt de data door de leverancier vernietigd.

3.3 Vastleggen en delen resultaten

Een red team hoort tot in detail vast te leggen wat ze heeft gedaan. De pogingen en resultaten worden op zo'n manier vastgelegd dat de oefening goed kan worden geëvalueerd. Ook voor het verbeteren van detectie is het essentieel dat dit gedetailleerd gebeurt; je wil de acties van het red team naast je (audit) logging kunnen leggen. Dit is niet een onderwerp om op te besparen. De volgende zaken worden gedeeld:

- Logboek: een beschrijving van de acties die het red team heeft uitgevoerd, met bijbehorende tijden. De red team mantra is: "Als er geen log is, hebben er geen acties plaatsgevonden.";
- Bewijsvoering: De verslaglegging van het red team moet gedetailleerd genoeg zijn (bijvoorbeeld met screenshots) om het blue team in staat te stellen om achteraf na te gaan wat wanneer gebeurd is en dat te correleren aan de signalen die ze op dat moment kregen;
- Presentatie/workshops achteraf (of, bij purple teaming, eventueel tussentijds).

3.4 Aanvalscenario's

Een van de zaken die na het tekenen van de offerte verder wordt afgestemd zijn de aanvalsscenario's en kroonjuwelen. Een goede leverancier zal hier het voortouw in nemen, eventueel met een gezamenlijke brainstorm. Als je voor het eerst een red teaming laat uitvoeren is het waarschijnlijk prima om de leverancier scenario's aan te laten dragen. Bij volgende tests wil je waarschijnlijk gerichter bepaalde systemen wel/niet meenemen (op basis van actuele dreigingsinformatie of kroonjuwelen), afhankelijk van het doel van je test.

3.5 Benodigdheden en leg-ups

Voor de meest realistische oefening gaat het red team zonder enige voorkennis of hulp aan de slag (ook wel een black box aanval genoemd). Voor de meeste organisaties zal het echter pragmatischer zijn om het red team alvast wat te vertellen over de ICT-omgeving en bij tegenvallende vooruitgang verder te helpen. Zo voorkom je bijvoorbeeld dat een red team weken moet blijven hangen in de 'IN' fase en weinig bevindingen over kroonjuwelen kan rapporteren. Een van de meest voorkomende leg-ups is dat het red team beschikking krijgt over een apparaat, een zogenaamde dropbox, in het netwerk, een beheerde laptop met inloggegevens (medewerker) of toegang tot een online werkomgeving (student). Het is belangrijk om deze benodigdheden van te voren af te stemmen, omdat het enige tijd kan duren om te regelen. Ook is het soms nodig om een domein of apparaat te allow-listen in beveiligingssoftware, ook dat wil je van tevoren weten.

3.6 Betrokkenen en het afdekken van escalatiepaden

Een ander onderwerp wat enige voorbereiding vergt zijn de hoeveelheid betrokkenen en de escalatiepaden. Je moet ervanuit gaan dat het red team ergens, soms meermaals, in de oefening wordt ontdekt en het nodig is om detecties te de-escaleren. Voor het realisme van de bevindingen is het echter belangrijk dat er zo normaal mogelijk gereageerd wordt op een detectie, en mensen niet op de hoogte hoeven worden gebracht dat er een oefening gaande is.

Voor de oefening moet je bedenken wie er betrokken en op de hoogte gaan zijn, in het white team of daarbuiten. Vaak is twee of drie mensen genoeg. Idealiter zitten deze mensen ook op plekken waar ze escalatie kunnen tegenhouden, zoals in een SOC, incident response team of in de organisatie er boven (bijvoorbeeld de CISO). Als het niet mogelijk is om een zekere scheiding tussen het white team en het blue team aan te houden, kan een purple-teaming opdracht beter passen omdat een red teaming snel waarde verliest als er veel detecties zijn of het red team vaak kunstmatig verder geholpen moet worden

Vooraf bespreek je met je red team provider wat voor soort detecties zouden kunnen voorkomen, en hoe aan de ene kant voorkomen wordt dat dat leidt tot grote bekendheid en onrealistische incident response, en aan de andere kant hoe voorkomen kan worden dat de voortgang van de oefening in gevaar komt.

3.7 Rules of engagement

Rules of Engagement zijn heldere afspraken die door de deelnemende partijen van tevoren worden vastgelegd. Hierdoor weet iedereen waar hij aan toe is en loopt de oefening, ook als er onvoorziene omstandigheden zijn, soepeler. Ook zijn er aan een red team oefening risico's verbonden, die je wilt beheersen door goede afspraken te maken. In de rules of engagement komen ook alle eerder beschreven afspraken over kaders, resultaten, scenario's, scope en benodigdheden terug.

De volgende zaken zou je moeten terugzien in de *Rules of Engagement*:

Doel van de oefening	Wat wordt getest? Welke scope is bepaald? Wat is het doel van de oefening?
Organisatie(onderdeel) in scope	Mogen ketenpartners worden aangevallen? Worden leveranciers betrokken? Hoe?
Kroonjuwelen	Welke kroonjuwelen of doelen wordt getracht tijdens de red team oefening toegang toe te krijgen? Dit bepaalt mede wanneer de oefening is afgerond.
Technische scope	Wat is de IP-range van de organisatie (om te voorkomen dat per ongeluk de verkeerde organisatie wordt gehackt)? Mag de procesautomatisering (OT) van de organisatie worden aangevallen?
Planning	Wanneer wordt de test uitgevoerd? Tijdens kantooruren of ook daarbuiten? Weekends? Feestdagen? Zijn er relevante *change windows* of andere redenen om op bepaalde dagen van de ICT af te blijven?
Wel en niet toegestane activiteit(en)	Mogen bijvoorbeeld fysieke middelen worden gebruikt?

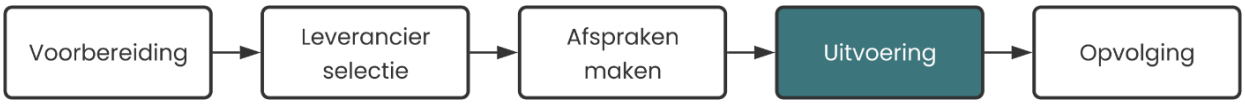
Wie is op de hoogte	Wie weten wel en wie weten niet dat de oefening plaatsvindt? (Zorg hierbij dat de juiste mensen op de hoogte zijn om snel te kunnen de-escaleren.)
Teams en contactinformatie	Om snel kunnen schakelen in voorziene en onvoorziene situaties. Neem ook op of SURF wel/niet bij het white team en de terugkoppeling betrokken is.
Communicatie	Zijn de helpdesk/SOC op de hoogte van de test? Zijn leveranciers op de hoogte? Wat is de frequentie van communiceren? Welke communicatiekanalen (regulier, escalatie)? Wat moet met wie gecommuniceerd, wat niet?
Vertrouwelijkheid	Welke informatie mag wel en niet uitgewisseld worden tussen de verschillende teams?
Escalatiepad	Wanneer gaat het white team escaleren? Waar ligt de beslissingsbevoegdheid voor een go/no go op vervolgacties?
Verslaglegging	Hoe en wanneer vindt verslaglegging plaats?
Voortijdig afbreken	Wanneer wordt de test afgebroken (denk aan calamiteiten, of het bekend worden van een zero-day tijdens de oefening)?

3.8 Checklist Afspraken maken

Maak de volgende afspraken met de leverancier:

- ☐ Wanneer start de oefening, wat is de doorlooptijd;
- ☐ Juridisch kader voor de oefening en de data: vrijwaringsverklaring, verwerkersovereenkomst, geheimhoudingsverklaring, bewaartermijnen;
- ☐ Hoe worden resultaten gedeeld;
- ☐ Wie zijn er (niet) op de hoogte van de oefening;
- ☐ Rules of engagement: hoe wordt de oefening uitgevoerd, wat mag wel en niet, hoe vindt de communicatie plaats;
- ☐ Wat moet de opdrachtgever (eventueel) aan hulp aanleveren voor en tijdens de oefening;
- ☐ Vastleggen van het escalatiepad.

4 Uitvoering



4.1 Red team

Het red team is aan het werk tijdens de uitvoering van de aanvalssimulatie. Zij voeren de aanval uit, binnen de afspraken die jullie met elkaar gemaakt hebben. Het red team verschaft het white team, de 'spelleiding', reguliere status updates.

4.2 White team

Het white team ziet toe op de juiste communicatie en stuurt bij waar dat nodig is:

- **Beheersen escalatie**. Als het white team observeert dat het blue team de activiteiten van het red team ontdekt heeft en gaat escaleren dient deze escalatie beheerd te worden – het white team zal het blue team op de hoogte stellen van de test. De test wordt niet afgebroken maar verandert van focus, aangezien het blue team er nu vanaf weet;
- **Leg-up**. Als de IN fase van de aanvalssimulatie te lang dreigt te duren is het verstandig om het red team toegang te geven om alsnog de THROUGH en OUT fases van de aanval uit te kunnen voeren. Hoewel het op zich goed nieuws is dat het team er niet in kwam, moeten we ervan uitgaan dat een aanvaller met voldoende geduld vroeg of laat altijd binnen zal komen;
- **High-risk fixen tijdens de uitvoering**. Het kan voorkomen dat tijdens de oefening kwetsbaarheden worden gevonden die directe actie vereisen. In dat geval zal het red team het white team op de hoogte brengen.

Kijk goed wie in het white team plaatsneemt. Veelal is dat de opdrachtgever. Gedacht kan worden aan bijvoorbeeld de CISO, of de verantwoordelijke directeur. Zorg ervoor dat het white team genoeg kennis heeft van de infrastructuur van de instelling. Voorbeeld: stel er worden rechten bemachtigd op een bepaald onderzoeksplatform, dan moet je als white team kunnen inschatten of het veilig genoeg is om het red team daar verder te laten gaan, of dat het te gevaarlijk is gezien het lopende onderzoek op dat platform. Zorg ook dat het white team voldoende bereikbaarheid heeft. Tijdens de uitvoering van de opdracht zal het red team zo nu en dan vragen stellen, een snelle respons helpt vaak in het efficiënt uitvoeren van de opdracht.

In overleg met SURF kan ook SURF bijdragen in het white team. Hiermee krijg je een extra persoon die reeds eerder ervaring heeft opgedaan met red teaming, die de sector goed kent en die meedenkt en suggesties kan geven voor de uitvoering. Dit helpt SURF ook om lessen te abstraheren die voor de sector beschikbaar gesteld kunnen worden (uiteraard geheel geanonimiseerd). Neem contact op met het SEC om afspraken te maken over de inzet van SURF.

4.3 Blue team

Het blue team probeert de aanval te detecteren. Het is een keus of het blue team van te voren op de hoogte wordt gebracht van een red team opdracht, of niet. Beide scenario's hebben voor- en nadelen:

- **Wel vertellen**: men voelt zich niet overvallen dat men aangevallen wordt. Dit kan namelijk overkomen als een check of ze het werk wel goed gedaan wordt. Dat is echter niet de focus van de oefening, die is om te kijken of er voldoende maatregelen zijn genomen. Door dit vooraf met het blue team te bespreken, kan de emotie tijdens een (geslaagde) aanval minder zijn. Uiteraard kan je nog kiezen hoe en wanneer je het verteld: we starten maandag om 09.00 uur, versus: we zijn van plan ergens dit jaar een red team uit te voeren.
- **Niet vertellen**: het is echt een verrassing en daarmee kan je kijken of de maatregelen die je hebt genomen ook echt werken. Immers, een echte hacker kondigt zichzelf ook niet vooraf aan. Hiermee zorg je dat het blue team niet opeens buitensporig veel aandacht gaat geven aan hele kleine signalen. Met als nadeel dat medewerkers zich overvallen kunnen voelen, zeker als ze bepaalde zaken willen escaleren waarbij het white team ze tegenhoudt om zodoende te kunnen kijken hoe ver het red team nog kan komen als de escalatie niet ingezet wordt.

Het uitvoeren van een red teaming heeft enkel zin indien er ook daadwerkelijk een blue team is. De uitgevoerde test komt tijdens het reguliere werk. En vormt ook een vorm van regulier werk: kijken of er inbreuken plaatsvinden. De activiteiten van het red team zullen tot acties van het blue team leiden. Houdt hier rekening mee, door bijvoorbeeld dit niet te plannen tijdens periodes van verminderde aanwezigheid van het blue team.

Houdt ook rekening met de escalatiepaden die doorlopen worden: ook daar zal een red teaming leiden tot inzet van interne medewerkers.

4.4 Delen uitkomsten

Als sluitstuk van een red team worden de rapportages opgeleverd. De bespreking van de detailrapportage met het blue team is het belangrijkste leermoment van de hele opdracht. Neem hier de tijd voor en zorg dat iedereen uit het blue en white team erbij is.

Zorg ook voor bespreking van de uitkomsten met het hogere management zodat zij een goed inzicht krijgen in de weerbaarheid van de instelling en de maatregelen die genomen moeten worden.

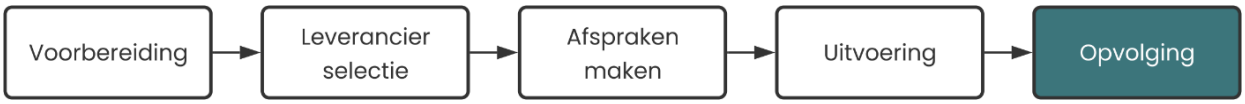
Kijk tot slot ook hoe de geleerde lessen breder gedeeld kunnen worden dan enkel binnen de eigen organisatie. Denk aan specifieke bijeenkomsten (TLP Red – achter gesloten deuren), via SCIPR of CISO overleggen. Ook wil SURF op basis van meerdere uitgevoerde red team opdrachten kijken of er bepaalde leerpunten vaker terugkomen. Om die vervolgens aan op geanonimiseerde wijze aan de hele sector mee te geven. Zo vergroot je niet alleen je eigen weerbaarheid, maar ook die van de hele sector! SURF ondersteund hier graag bij, neem daarvoor contact op met het SEC.

4.5 Checklist Uitvoering

Let bij de uitvoering op de volgende zaken:

- ☐ Communicatie via white team;
- ☐ Escalatie als nodig – blue team ontdekt de aanval voortijdig;
- ☐ Leg up – red team heeft hulp nodig bij IN fase;
- ☐ High risk fixen – red team vindt een kwetsbaarheid die directe actie vereist.

5 Opvolging



Een red team oefening wordt afgesloten met kennisoverdracht. Het doel is immers om te leren van de oefening. Na afloop vindt dan ook een bespreking met het blue team plaats. De vorm en diepgang van deze bespreking is van tevoren afgesproken. Het kan een rapport of presentatie zijn (een presentatie is levendiger, interactiever en kun je niet in de la stoppen), maar ook een meerdaagse workshop in het geval van een purple team oefening.

Het red team laat sporen achter op het netwerk: malware, sessies, instellingen. Ze leveren hier na afloop een overzicht van zodat de organisatie dit kan opruimen. Dit kost de opdrachtgever achteraf tijd, die ook ingepland dient te worden.

5.1 Het vervolg

Behalve een bespreking met het Blue Team zullen - ook op directieniveau – nog meer acties moeten plaatsvinden om de lessen van de oefening optimaal te benutten:

- **Interne evaluatie:** wat heeft de red team oefening opgeleverd, wat hadden we verwacht en waar schrokken we van? Wat hebben we geleerd? Omdat een red team oefening als voornaamste doel heeft om de organisatie te verbeteren dient de oefening altijd gekoppeld te worden aan een gedegen evaluatie. Zonder zo'n evaluatie gaat een groot deel van het leereffect verloren;
- **Opvolging resultaten:** de resultaten van de red team oefening zijn de basis voor acties die de opdrachtgever zal moeten uitvoeren om het securityniveau te verhogen. Zonder deze acties is het nut van een red team oefening beperkt. De uitkomsten van de red team oefening worden naast de Security Roadmap gelegd en deze wordt geüpdatet waar dat nodig is;
- **Lessons learned delen:** laat de lessen van de red team oefening niet binnen het kleine gremium blijven waarin het is uitgevoerd. De uitkomsten van de red team oefening kunnen gebruikt worden als basis om awareness te creëren, zowel bij de directie als organisatiebreed.

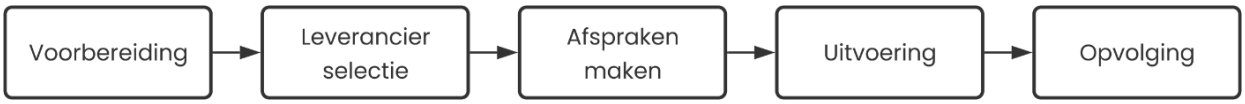
Deel de lessen ook extern, met partnerorganisaties of in de sector. Denk aan specifieke bijeenkomsten (TLP Red – achter gesloten deuren), **SCIRT in TLP:RED rondje**, maar ook SCIPR of CISO overleggen zijn hier uitermate geschikt voor. Er zijn te veel aanvallen om op security te concurreren. Vroeg of laat krijgt elke organisatie met een aanval te maken. Het delen van de geleerde lessen maakt onze samenleving als geheel weerbaarder. Het aantal organisaties met angst om (gefixte) kwetsbaarheden te delen neemt gelukkig af; delen is juist een teken van een volwassen organisatie. Ook wil SURF op basis van meerdere uitgevoerde red team opdrachten kijken of er bepaalde leerpunten vaker terugkomen. Om die vervolgens aan op geanonimiseerde wijze aan de hele sector mee te geven. Zo vergroot je niet alleen je eigen weerbaarheid, maar ook die van de hele sector! SURF ondersteunt hier graag bij, neem daarvoor contact op met het SEC.

5.2 Checklist Opvolging

Na de uitvoering start de opvolging met:

- ☐ Kennisoverdracht – verslaglegging / presentatie van het red team;
- ☐ Evaluatie – wat heeft de oefening voor de organisatie opgeleverd;
- ☐ Acties – wat moeten we doen naar aanleiding van de uitkomsten;
- ☐ Opruimen van de sporen van de oefening;
- ☐ Uitdragen – lessons learned delen binnen en buiten de organisatie.

6 Checklist Red Teaming



6.1 Voorbereiding

Voor je begint aan een red team oefening dien je op de volgende vragen antwoord te kunnen geven.

- ☐ Wat is het doel van de oefening?
- ☐ Wat is het dreigingsbeeld voor mijn instelling?
- ☐ Wat zijn goede potentiële aanvalsscenario's?
- ☐ Welke vorm van red team oefening sluit het beste aan bij mijn doel?
- ☐ Welke aanvalsvormen wil ik uitsluiten?
- ☐ Wat zijn de kroonjuwelen van mijn organisatie?
- ☐ Welke maatregelen heb ik genomen om ze te beschermen?
- ☐ Wat is mijn gewenste eindresultaat van de red team oefening?
- ☐ Wat is mijn budget?
- ☐ Wanneer mag de oefening starten, hoelang mag ze duren, wanneer mag niet geoefend worden?

6.2 Leverancier selectie

Let bij het kiezen van een geschikte leverancier op de volgende zaken:

- ☐ Vraag de aanbieder naar het huidige dreigingsbeeld;
- ☐ Vraag de aanbieder om een voorbeeldrapportage;
- ☐ Vraag de aanbieder welk kader hij gebruikt om de scenario's aan op te hangen;
- ☐ Vraag de aanbieder hoe zij voor realistische scenario's zorgen, of hoe ze daarbij helpen;
- ☐ Vraag de aanbieder naar een generiek scenario;
- ☐ Vraag de aanbieder zijn competentie aan te tonen;
- ☐ Heeft de aanbieder de test en de tijdsduur helder en onderbouwd omschreven?
- ☐ Zijn er afspraken te maken over het omgaan met gevoelige informatie?
- ☐ Zijn prijs en kwaliteit in balans?
- ☐ Nodig de aanbieder uit zijn offerte toe te lichten en vragen te beantwoorden.

6.3 Afspraken maken

Maak de volgende afspraken met de leverancier:

- ☐ Wanneer start de oefening, wat is de doorlooptijd;
- ☐ Juridisch kader voor de oefening en de data: vrijwaringsverklaring, verwerkersovereenkomst, geheimhoudingsverklaring, bewaartermijnen;
- ☐ Hoe worden resultaten gedeeld;
- ☐ Wie zijn er (niet) op de hoogte van de oefening;
- ☐ Rules of engagement: hoe wordt de oefening uitgevoerd, wat mag wel en niet, hoe vindt de communicatie plaats;
- ☐ Wat moet de opdrachtgever (eventueel) aan hulp aanleveren voor en tijdens de oefening;
- ☐ Vastleggen van het escalatiepad.

6.4 Uitvoering

Let bij de uitvoering op de volgende zaken:

- ☐ Communicatie via white team;
- ☐ Escalatie als nodig – blue team ontdekt de aanval voortijdig;
- ☐ Leg up – red team heeft hulp nodig bij IN fase;
- ☐ High risk fixen – red team vindt een kwetsbaarheid die directe actie vereist.

6.5 Opvolging

Na de uitvoering start de opvolging met:

- ☐ Kennisoverdracht – verslaglegging / presentatie van het red team;
- ☐ Evaluatie – wat heeft de oefening voor de organisatie opgeleverd;
- ☐ Acties – wat moeten we doen naar aanleiding van de uitkomsten;
- ☐ Opruimen van de sporen van de oefening;
- ☐ Uitdragen – lessons learned delen binnen en buiten de organisatie.