Voorstel penetratietesten

All Automation Service

Datum: 09 oktober 2024
Auteur: R. Hulzinga
Referentie: ALLAS_PEN_102024_V1.0

RedTeam Cyber Security B.V.
Meander 901
6825 MH Arnhem

T: +31 26 20 22 028
I: www.redteam-security.nl

RedTeam CYBER SECURITY
A OneXillium Group Company

All Automation Service

Voorwoord

Geautomatiseerde informatie-uitwisseling en verwerking is binnen organisaties inmiddels verweven in alle processen en niet meer weg te denken zonder dat het tot schade kan leiden. De afhankelijkheid van correcte en kwalitatief goede informatieprocessen is dan ook zeer groot geworden en zal in de toekomst naar verwachting alleen nog maar groter zijn. Organisaties, klanten en burgers moeten er daarom op kunnen vertrouwen dat de beveiliging van gegevens op een juiste wijze wordt toegepast. De woorden ‘vertrouwen’ en ‘mens’ vervullen hierin een sleutelrol.

De continu veranderende ICT-wereld, de evenredig mee veranderende dreigingen en risico’s en de wet en regelgevingen waaraan voldaan moet worden zorgen ervoor dat informatiebeveiliging een complex specialisme is geworden waarin RedTeam zich heeft bekwaamd. De verantwoordelijkheid over informatiebeveiliging blijft een aangelegenheid van directie, management en medewerkers. Maar het verkrijgen van de kennis en vaardigheden om passende maatregelen te treffen is niet iets wat je ‘er even bij’ kunt doen. ‘Schoenmaker blijf bij je leest’ is ook in dit geval een klassiek maar treffend gezegde omdat het niet goed herkennen van risico’s en dreigingen of het niet goed toepassen van maatregelen kan veroorzaken dat er financiële, imago- of zelfs persoonlijke schade ontstaat.

RedTeam heeft een goede naam opgebouwd in de specialistische wereld van informatiebeveiliging. Bij de aanpak van beveiligingsprojecten staat altijd de mens, als cruciale schakel in beveiliging, centraal tezamen met de bedrijfsprocessen van de opdrachtgever. Informatiebeveiliging wordt op deze manier ondersteunend en ingezet als een ‘business enabler’ en niet als een noodzakelijk kwaad en kostenpost.
RedTeam stelt zich tot doel de zorgen van de opdrachtgever over de complexe wereld van informatiebeveiliging uit handen te nemen zodat beveiliging begrijpelijk en beheersbaar wordt.

Inhoudsopgave

1 Inleiding | vraagstelling

All Automation Service bied al meer dan 33 jaar de beste service op het gebied van automatisering en zijn dé IT partner van diverse organisaties in het MKB. All Automation Service heeft kennis en ervaring met zowel netwerkbeheer, systeembeheer (Windows en Linux), cybersecurity, webdevelopment en softwareontwikkeling. Daarnaast bieden All Automation Service op maat gemaakte ICT diensten en oplossingen voor zowel 'on-premise' en cloud omgevingen.

All Automation Service heeft tijdens het scopegesprek op [DATUM] RedTeam Cyber Security (hierna RedTeam) gevraagd een voorstel uit te brengen voor het uitvoeren van penetratietesten.
Bij dit scope gesprek waren aanwezig:

- Bob, namens All Automation Service;
- Aaron, namens All Automation Service;
- Sait, namens RedTeam;
- Richard, namens RedTeam.

All Automation Service wil haar klanten de mogelijkheid bieden om een penetratietest te laten uitvoeren op de interne IT-infrastructuur, waarbij naast de kwetsbaarheden ook onderzocht wordt of het All Automation Service SOC goed en adequaat reageert.

Per klant zal afgestemd worden wat de onderzoeksvragen zijn en zal er een voorstel worden gemaakt.

Belangrijk is dat de opdracht time-boxed wordt uitgevoerd, wat wil zeggen dat een consultant van RedTeam 1 dag op locatie komt om te testen en daarnaast korte lijnen ook houdt met het SOC-team van All Automation Service.

2 Beantwoording

RedTeam doet hierbij een voorstel voor penetratietesten, waarbij RedTeam de volgende type penetratietest gaat uitvoeren zoals hieronder omschreven.

Interne IT-infrastructuur

RedTeam zal een zogeheten “Assume Breach” aanpak hanteren op de interne IT infrastructuur. Deze methodiek simuleert een scenario waarbij een aanvaller toegang heeft tot een systeem binnen het interne netwerk Van de klant van All Automation Service bijvoorbeeld als gevolg van een phishing aanval, waarmee de aanvaller toegang heeft tot het werkstation van het slachtoffer. De consultant komt op locatie bij de klant van All Automation Service. De laptop van de consultant wordt aangesloten op het door de klant van All Automation Service gekozen netwerksegment. Door misbruik te maken van kwetsbaarheden en misconfiguraties probeert de consultant zich in het netwerk te nestelen en te escaleren naar systemen en accounts die meer rechten bezitten. Uiteindelijke doel: domein administrator rechten verkrijgen. De klant van All Automation Service levert hiervoor inloggegevens aan van een account met lage privileges.

Rapportage

De rapportage wordt opgemaakt in het Nederlands en bevat een managementsamenvatting en een technisch deel. Daarna volgt de rapportage bespreking waarin RedTeam alle bevindingen extra toelicht en mogelijke vragen beantwoord.

Bij kritieke bevindingen tijdens het onderzoek zal RedTeam direct contact opnemen met de door All Automation Service opgegeven technisch contactpersoon welke tijdens de testen bereikbaar is. De contactgegevens worden opgenomen in de vrijwarings- en geheimhoudingsovereenkomst.

3 Scope

Dit onderdeel beschrijft de scope waar All Automation Service de penetratietesten op wil laten uitvoeren. Onderstaande tabel geeft een overzicht van de doelwitten en de testmethodiek.

Omschrijving	Locatie	Testmethode
Interne IT-infrastructuur klant All Automation Service	Intern bij klant All Automation Service	Time-boxed Greybox (Assume breach scenario)

De exacte scope wordt opgenomen in de vrijwarings- en geheimhoudingsovereenkomst. RedTeam zal alleen de IP-ranges en URL's testen die in de vrijwarings- en geheimhoudingsovereenkomst zijn opgenomen. RedTeam is niet verantwoordelijk voor de scope bepaling.

4 Planning

Datum (doorlooptijd)	Wie	Activiteit
Nader te bepalen	All Automation Service + RedTeam	Akkoord offerte + tekenen vrijwarings- en geheimhoudingsovereenkomst
Nader te bepalen	All Automation Service + RedTeam	Kick-off meeting
Nader te bepalen	RedTeam	Uitvoeren penetratietesten
Nader te bepalen	RedTeam	Rapportage opmaken
Nader te bepalen	All Automation Service + RedTeam	Rapportage bespreken
Nader te bepalen	All Automation Service + RedTeam	Voortgang bespreken

Wanneer All Automation Service en RedTeam tot een overeengekomen definitieve planning zijn gekomen, kan deze planning tot 10 werkdagen voor de uitvoering van de overeengekomen ingeplande werkzaamheden, zonder extra kosten opnieuw worden ingepland. Is dit termijn echter korter, dan kan RedTeam de werkzaamheden geheel (100%) of gedeeltelijk (50%) in rekening brengen. Uiteraard doen we alles eraan om dit te voorkomen.

5 Waarom RedTeam Cyber Security

- + Gecertificeerd voor het CCV-keurmerk pentesten
- + Korte lijnen ‣ single point of contact
- + Duidelijk Plan van Aanpak
- + Een volledig TEAM per opdracht ‣ dus niet één individuele consultant
- + In teamverband werken geeft meer inzichten
- + Verbanden herkennen ‣ door de enorme bagage aan ervaring die wij met ons meenemen
- + Regionaal ‣ we zitten in de buurt
- + Gezamenlijk de situatie verbeteren ‣ samen met de klant naar de toekomst kijken
- + Integer personeel ‣ gescreend op minimaal VOG-niveau en de helft van de medewerkers ook op AIVD-B
- + Gecertificeerd personeel ‣ o.a. OSCP, OSCE, SANS GPEN, CISSP en CEH
- + Vrijwarings- en geheimhoudingsovereenkomst ‣ zonder starten wij niet
- + Rapportages bevatten een volwaardig advies
- + Rapportages worden gepresenteerd en met u besproken
- + Competitief

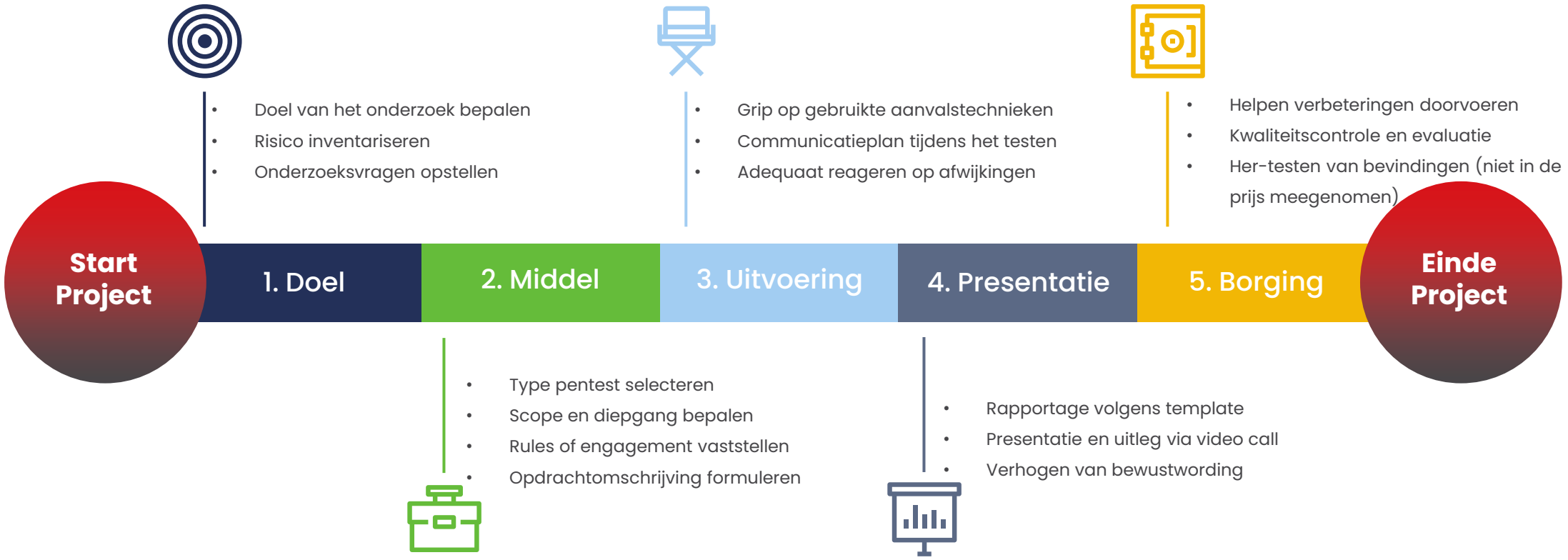
RedTeam Cyber Security heeft diverse belangrijke prijzen gewonnen bij recente wedstrijden, zoals de 1e prijs bij het hackers event “Hack den Haag” in 2019, een 2e prijs bij het KPN Secure-ID-event begin 2020 en recent tijdens ”Hack The Hague 21” een prijs in de categorie “most impactful hack”. RedTeam is regelmatig te vinden bij security conferenties in Nederland en sponsort goede initiatieven om Nederland veilig te maken.

CCV CYBER PENTEST

6 Plan van aanpak penetratietesten

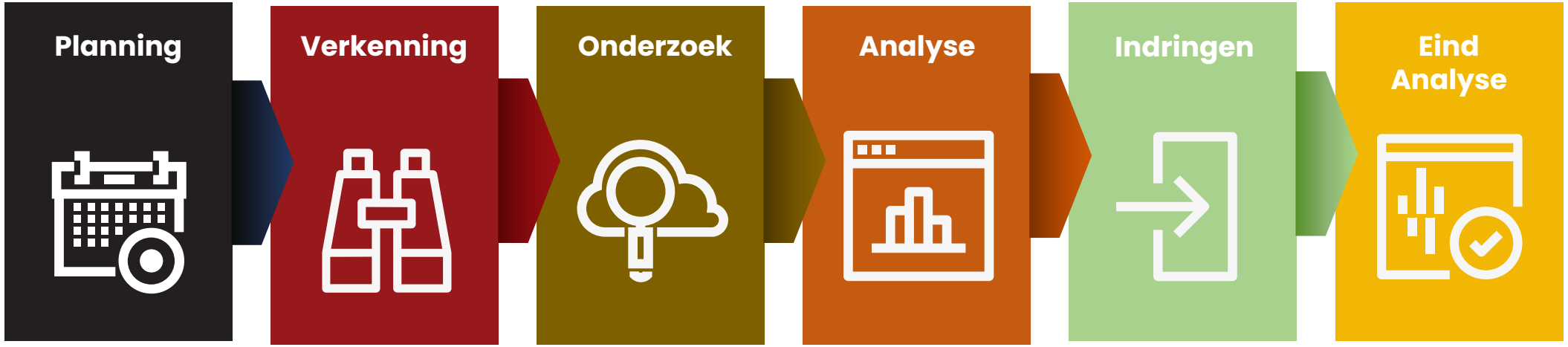
6.1 Stappenplan

Penetratietesten doorlopen over het algemeen de volgende stappen zoals weergegeven in het onderstaande overzicht, een uitgebreide beschrijving van de stappen is te vinden in hoofdstuk 9 “Plan van aanpak (uitgebreid)”:



6.2 Testmethodiek

RedTeam gebruikt de volgende methodologie om de penetratietest uit te voeren, zoals weergegeven in het onderstaande diagram, een uitgebreide beschrijving van de methodiek is te vinden in hoofdstuk 10 "Testmethodiek (uitgebreid)":



7 Investering

Deze offerte geeft een overzicht van de investering per activiteit en heeft een geldigheid van vier weken gerekend vanaf de datum van verzending. Op deze aanbieding zijn de algemene voorwaarden van RedTeam Cyber Security B.V. van toepassing.

Nadat de penetratietest is uitgevoerd en de bevindingen bekend zijn kunt u aan de slag om deze op te (laten) lossen. Als de bevindingen zijn gemitigeerd adviseren wij een her-test (niet in de prijs meegenomen) uit te voeren om vast te stellen of dit daadwerkelijk goed is gebeurd. Een penetratietest is een momentopname en daarom adviseren wij om minimaal één keer per jaar een penetratietest te laten uitvoeren.

Voor het uitvoeren van de opdracht zoals beschreven, hanteert RedTeam een geheimhouding en behandelt deze opdracht en alle informatie die voortvloeit uit deze opdracht als vertrouwelijk.

Deze opdracht wordt time-boxed uitgevoerd. Mocht tijdens de uitvoering blijken dat de scope anders is dan vooraf is aangenomen dan zullen wij dit tijdig bij u aangeven en kan er bepaald worden of er meer of minder inzet nodig is.

Component		Prijs
Penetratietest interne IT-infrastructuur Time-boxed 8 uur onderzoek + 8 uur restant	€	2.400,-
• Scoping • Kick-off • Greybox methodiek (Assume breach scenario) **8 uur** • Opmaken Rapportage • Presentatie Rapportage • Kwaliteitsmanagement • Projectmanagement		
Totaal	€	2.400,-

Alle prijzen zijn exclusief BTW en inclusief reiskosten binnen Nederland
Betalingstermijn: 30 dagen

8 Opdrachtbevestiging

Indien All Automation Service zich kan vinden in het aanbod van deze offerte, dan verzoeken wij u de opdracht te bevestigen door het terugsturen van de getekende offerte. Met de ondertekening verklaart u tevens tekenbevoegd te zijn voor het aangaan van deze offerte. Tevens bevestigd u met uw ondertekening akkoord te gaan met de algemene voorwaarden van RedTeam Cyber Security B.V. die op deze opdracht van toepassing zijn.

Opdrachtnemer:

RedTeam Cyber Security B.V.

Handtekening:

Datum:

Naam:

Functie:

RedTeam Cyber Security B.V.

Opdrachtgever:

All Automation Service B.V.

Handtekening:

Datum:

Naam:

Functie:

Factuur mailadres:

Uitgebreide beschrijvingen

- Plan van aanpak
- Methodiek
- Integriteit en screening medewerkers
- Ingezette kwaliteitsnormen

9 Plan van aanpak (uitgebreid)

9.1 Doel

Samen bepalen we wat er precies beschermd moet worden en welke inzichten daarbij nu ontbreken.

We stellen in deze fase kritische vragen om te zorgen dat het juiste getest wordt. Het helpt om een onderzoeksvraag te formuleren om het doel helder te krijgen.

Voorbeelden van onderzoeksvragen zijn:

- Is het mogelijk om ongeautoriseerd toegang tot het te onderzoeken systeem te krijgen?
- Is het mogelijk om toegang te verkrijgen tot gevoelige informatie?
- Is het mogelijk om fysieke toegang te verkrijgen tot locaties en/of afgesloten ruimtes?
- Is het mogelijk om eindgebruiker en/of beheerder accounts te bemachtigen?
- Is het mogelijk om langdurige (onopgemerkte) toegang te verkrijgen?

Deze stap wordt meestal in een dialoog gecombineerd met de vormgeving in stap 2, “Middel”.

9.2 Middel

In deze stap bepalen we het type security test en welke opties het best passen bij de situatie en het doel. Dit kan een systeem specifieke test zijn of een scenario gedreven test. In elke test is het mogelijk om het perspectief en vertrekpunt van de test te bepalen dat als uitgangspunt zal worden gehanteerd voor de test.

Per test stemmen wij gezamenlijk af welke rules of engagement worden toegepast. In deze rules of engagement maken wij afspraken hoe wij omgaan met:

- Betrokkenen, met een rol in het communicatieplan;
- Wanneer de test plaats gaat vinden;
- Of de test vooraf wel of niet wordt aangekondigd;
- Debriefing of presentatie van de bevindingen;
- Bepalen of beveiligingsmaatregelen actief zijn tijdens test of worden uitgeschakeld;
- Bepalen of er situaties zijn waarbij de test moet worden gestaakt;
- Aanvalstechnieken die minimaal worden ingezet tijdens de test;
- Technische inrichting, welke systemen en rand apparatuur worden gebruikt;
- Bepalen wie controle uitvoert of detectiemaatregelen zoals logging en monitoring succesvol zijn geweest in het detecteren van alarmen;
- vrijwarings- en geheimhoudingsovereenkomst ondertekend door beide partijen.

Al naar gelang de behoefte worden deze regels aangevuld met relevante vragen uit de pentest execution standard2.

Deze fase wordt afgesloten met een opdrachtomschrijving in de vorm van een document. Deze omvat de onderzoeksvraag, de uitwerking van de rules of engagement, gebruikte aanvalstechnieken, een communicatieplan, planning en een getekende vrijwarings- en geheimhoudingsovereenkomst.

Zonder een getekende vrijwarings- en geheimhoudingsovereenkomst door de tekenbevoegde, kan de volgende fase niet starten.

9.3 Uitvoering

In deze stap volgt de uitvoering van de penetratietest. De belangrijkste onderdelen van deze stap is het volgen van de gemaakte afspraken.

Mocht er zich onverhoopt een belemmering of incident voordoen aan de kant van de opdrachtgever of opdrachtnemer, dan wordt volgens de afspraken naar een passende oplossing of alternatief gezocht. RedTeam houdt voldoende pentesters beschikbaar om uitloop of uitval op te vangen. Welke personen er dan worden ingezet beschrijven wij in het communicatieplan.

Tijdens de uitvoering kan via monitoring worden gecontroleerd of de opdracht conform afspraak wordt uitgevoerd. RedTeam verzamelt daarnaast van alle bevindingen en tests bewijsmateriaal dat wordt bewaard en tot de oplevering van het rapport. Na overdracht van alle informatie verwijderen wij alle klantdata van onze systemen.

9.4 Presentatie

Alle bevindingen en resultaten van de test en analyses worden opgetekend in een schriftelijke rapportage in het Nederlands. Het rapport bevat een managementsamenvatting, een beschrijvend en een technisch deel.

De rapportage heeft als doel een duidelijk overzicht te geven in de staat van beveiliging. We maken duidelijk waar de kwetsbaarheden en risico's zich bevinden en we geven maatregelen en verbeter acties aan die de risico's beperken of weg nemen. Bij elke aanbeveling is een prioriteit toegekend. De prioriteitsaanduiding is gebaseerd op de ernst van de kwetsbaarheid en de kans van optreden van uitbuiting. De rapportage sluit af met een conclusie en een advies,

Vervolgens plannen we een debriefing samen met de betrokkenen. De vorm en frequentie van deze presentatie is afgestemd in de "middel" fase. Er zijn hier tal van vormen mogelijk, maar de meest gebruikte is bij voorkeur een presentatie op locatie of een video conferentie met:

- Een bondige managementsamenvatting aan de CISO en directie;
- Risico's en aanbevolen strategie leggen we voor aan de security officer;
- De inhoudelijke technische zaken wordt met beheerders en ontwikkelaars gedeeld.

Onze pentesters delen graag kennis over de bevindingen en geven advies over mogelijke oplossingen en de inspanning die hiervoor nodig is. We stellen op verzoek een (deel)opname van de presentatie beschikbaar voor de interne security awareness trainingen of het intranet.

9.5 Borging

Wanneer de testen zijn uitgevoerd en de kennis is overgedragen over hoe de bevindingen moeten worden opgelost volgt een fase van herstel werkzaamheden. Als de herstelwerkzaamheden zijn uitgevoerd is het raadzaam om door een her-test aan te laten tonen of de gevonden risico's succesvol zijn gemitigeerd.

Om een zo hoog mogelijke kwaliteit te behalen voeren we na elke test een evaluatie uit. We horen graag wat goed ging maar ook wat beter kan en nemen deze lessen mee naar de volgende test. Communicatie is belangrijk en goed luisteren naar elkaar en bijsturen indien nodig zal bijdragen aan een prettige samenwerking.

Het uitvoeren van een pentest en daarbij aanbevelingen geven voor verbetering is waar wij goed in zijn. Als wij meerdere pentesten uitvoeren bij dezelfde klanten geven de resultaten van meerdere testen ons inzicht in waar structurele verbeteringen liggen.

Onze meerwaarde leveren wij door een overzicht hiervan te maken en de problematiek inzichtelijk te maken bij de basis in plaats van het plakken van een pleister op een lek dat in meerdere pentesten terugkomt. Wij doen dit via een presentatie bij meer klanten en krijgen hier goeie feedback op. Wij zetten graag een stap extra en willen onze klanten écht helpen veiliger te worden..

10 Testmethodiek

10.1 Plan

Planning en voorbereiding begint met het definiëren van de doelen en doelstellingen van de penetratietesten. All Automation Service en RedTeam hebben gezamenlijk de doelen gedefinieerd, zodat beide partijen dezelfde doelen en hetzelfde begrip hebben. De gemeenschappelijke doelstellingen van penetratietesten zijn het identificeren van de kwetsbaarheid en het verbeteren van de beveiliging van de technische systemen. .

10.2 Verkenning

Verkenning omvat een analyse van de voorlopige informatie. Het IP-adres of IP-adresblok wordt geanalyseerd op administratieve correctheid en vergeleken met open source intelligence-databases. Het enige doel is om volledige en gedetailleerde informatie over de systemen te verkrijgen.

10.3 Onderzoek

Onderzoek, in deze stap gebruikt RedTeam handmatige en geautomatiseerde tools om doelactiva te scannen om kwetsbaarheden te ontdekken. Alle resultaten van alle tools worden gecombineerd in één overzicht en geverifieerd.

10.4 Analyse

De analyse van informatie en risico's. In deze stap analyseert en beoordeelt RedTeam de informatie die vóór de teststappen is verzameld om het systeem dynamisch te penetreren. Vanwege het grotere aantal systemen en de omvang van de infrastructuur, kan dit tijdrovend zijn. Bij het analyseren wordt rekening gehouden met de gedefinieerde doelen van de penetratietest en het mogelijke risico voor het systeem.

10.5 Indringen

Deze fase is voor het actief indringen (binnendringen). Dit is de belangrijkste stap die met zorg moet worden uitgevoerd. Deze stap houdt in, in hoeverre de potentiële kwetsbaarheden die in de ontdekkingsstap zijn geïdentificeerd, de daadwerkelijke risico's bevatten. Deze stap moet worden uitgevoerd wanneer een verificatie van mogelijke kwetsbaarheden nodig is. Voor die systemen met zeer hoge integriteitsvereisten, moet de potentiële kwetsbaarheid en het risico zorgvuldig worden overwogen voordat kritieke opschoningsprocedures worden uitgevoerd.

10.6 Eind analyse

In deze stap wordt primair gekeken naar alle uitgevoerde stappen en wordt een evaluatie van de kwetsbaarheden gepresenteerd in de vorm van mogelijke risico's. Verder worden aanbevelingen toegevoegd om de kwetsbaarheden en risico's weg te nemen.

11 Integriteit en screening medewerkers

De medewerkers van RedTeam worden voordat zij in dienst komen gescreend en referenties worden nagetrokken. Er wordt onderzoek gedaan naar de digitale footprint en Social Media. Ook worden diploma's nagetrokken.

Voor iedere medewerker wordt een VOG opgevraagd bij in dienst treden met in ieder geval de minimale functieaspecten:

- 11: Bevoegdheid hebben tot het raadplegen en/of bewerken van systemen;
- 12: Met gevoelige/vertrouwelijke informatie omgaan;
- 41: Het verlenen van diensten (advies, beveiliging, schoonmaak, catering, onderhoud, etc.).

Twee jaarlijks wordt er een nieuwe VOG opgevraagd. Daarnaast kunnen wij op aanvraag van de opdrachtgever een actuele VOG opvragen met de daarbij behorende risicogebieden welke voor de opdrachtgever vereist zijn en deze overhandigen.

De helft van de medewerkers is AIVD gescreend ten behoeve van de werkzaamheden voor specifieke opdrachtgevers.

Ook wordt er door alle medewerkers een NDA getekend bij indiensttreding als toevoeging op de arbeidsovereenkomst.

Daarnaast tekenen wij bij iedere opdracht een vrijwarings- en geheimhoudingsovereenkomst. RedTeam begint niet aan de opdracht als deze documenten niet ondertekend zijn door de opdrachtgever.

12 Ingezette kwaliteitsnormen

De kwaliteit van het onderzoek wordt in grote mate bepaald door de mate van expertise en ervaring van de uitvoerende securityspecialisten in combinatie met gestructureerd werken.

Expertise

De opdracht wordt uitgevoerd door een team van professionals, een gebalanceerde mix van talent en ervaring. Het team is voor pentesten gecertificeerd op expert niveau, o.a.:

- Offensive Security Certified Professional (OSCP);
- Offensive Security Experienced Penetration Tester (OSEP);
- Offensive Security Certified Expert (OSCE);
- Offensive Security Web Expert (OSWE).

Samen wint het team regelmatig nationale hack competities en vinden ze dagelijks nieuwe kwetsbaarheden bij gelijkwaardige organisaties zoals die van u.

Volledigheid

Het team voert pentesten op gestructureerde wijze uit.
Hierbij wordt een methodologie gebruikt welke is afgeleid van internationaal hiervoor erkende standaarden:

- NIST 800-115
- Penetration Execution Standard (PTES)
- Open Web Application Security Project (OWASP)

Om de kwetsbaarheden in risico categorieën te classificeren wordt het Common Vulnerability Scoring System (CVSS) versie 4.0 gehanteerd om de mate van ernst van de bevindingen inzichtelijk te maken.
Het MITRE-attack framework is de leidraad voor selectie van technieken waarmee de verschillende fasen van een aanval worden doorlopen.

Kwaliteitscontrole

RedTeam zet meerdere consultants in per opdracht. Dit leidt tot meer en verschillende inzichten en stimuleert de creativiteit, wat uiteindelijk ten goede komt van de kwaliteit.

RedTeam voert kwaliteitscontrole uit op de rapportages, onderdelen van deze kwaliteitscontrole zijn:

- Controle op volledigheid scope, is alles uitgevoerd?;
- Review door andere consultant (4 ogen principe);
- Is de boodschap in zowel de managementsamenvatting als het technische deel duidelijk verwoord;
- Eindbeoordeling door een senior consultant.

CCV-certificatieschema cybersecurity pentesten

RedTeam Cyber Security is officieel gecertificeerd door het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV).

Het CCV-keurmerk pentesten, gebaseerd op de NEN-EN-ISO/IEC-normen 17021 en 17065, zorgt voor geborgde kwaliteit van pentesten. Doordat wij gecertificeerd zijn volgens het CCV-certificatieschema Cybersecurity Pentesten kunnen wij bij onze klanten aantonen dat een geleverde test voldoet aan de geldende kwaliteitseisen.

Bijlagen

- Bijlage A: Ervaring
- Bijlage B: Vrijwarings- en geheimhoudingsovereenkomst

Bijlage A: Ervaring

Hieronder een selectie van enkele organisaties waar RedTeam pentest ervaring heeft:

Bijlage B: Vrijwarings- en geheimhoudingsovereenkomst

Voor de uitvoering van de security penetratietest (hierna: 'pentest'), zoals nader omschreven in het Voorstel penetratietesten, is het noodzakelijk dat de opdrachtgever en RedTeam Cyber Security B.V. (hierna: 'RedTeam') deze vrijwarings- en geheimhoudingsovereenkomst ondertekenen. Een pentest kan namelijk tot schade leiden bij de opdrachtgever.

Door ondertekening stemmen beide partijen in met het volgende:

Artikel 1: Opdracht

1.1 De opdrachtgever geeft aan RedTeam toestemming om bij hem een pentest uit te voeren, zoals nader omschreven in het Voorstel penetratietesten. Bij de uitvoering van de pentest zal RedTeam in ieder geval proberen zich digitaal toegang te verschaffen tot de ICT-systemen van de opdrachtgever om inzicht te krijgen in de actuele staat van het beveiligingsniveau en de kwetsbaarheden van de onderzochte ICT-systemen. Ook zal RedTeam proberen te identificeren welke gegevens mogelijk toegankelijk zijn voor personen die wederrechtelijk binnendringen op de ICT-systemen van de opdrachtgever.

1.2 RedTeam zal de resultaten ten aanzien van de pentest rapporteren aan de opdrachtgever door, al dan niet met behulp van een rapportagesoftware, een rapportage voor opdrachtgever op te stellen en aan hem te verstrekken.

1.3 Naast de in het vorige lid genoemde rapportage kan opdrachtgever ook een klantportaal applicatie van RedTeam afnemen. De bevindingen van RedTeam naar aanleiding van de pentest zullen in de klantportaal applicatie, onder meer in de vorm van een dashboard, worden weergegeven.

1.4 Het herstel van de geconstateerde kwetsbaarheden is geen onderdeel van de tussen de opdrachtgever en RedTeam gesloten overeenkomst. De opdrachtgever dient zelf zorg te dragen voor het herstel van de betreffende kwetsbaarheden. Ook is de opdrachtgever te allen tijde zelf verantwoordelijk om artefacten en/of restanten van de pentest te verwijderen uit zijn ICT-systemen en/of computernetwerken.

1.5 Het maken van een back-up van de gegevens van de opdrachtgever is geen onderdeel van de tussen de opdrachtgever en RedTeam gesloten overeenkomst. Opdrachtgever dient te allen tijde zelf zorg te dragen voor een volledige back-up van alle gegevens die op zijn of door hem gebruikte ICT-systemen en/of computernetwerken zijn opgeslagen.

Artikel 2: Vrijwaring en aansprakelijkheid

2.1 In het kader van de pentest voert RedTeam activiteiten uit waarbij de beveiliging van de ICT-systemen en/of computernetwerken van opdrachtgever mogelijk wordt doorbroken, omzeild en/of toegang wordt verworven tot deze systemen met behulp van valse signalen of valse sleutel dan wel een valse identiteit wordt aangenomen. RedTeam voert deze handelingen uit in opdracht en op verzoek van de opdrachtgever. De opdrachtgever vrijwaart RedTeam dan ook tegen aansprakelijkheden dienaangaande, met name ingeval een derde zich beroept op de artikelen 161 sexies, 161 septies, 351, 351 bis 138ab of 138b Wetboek van Strafrecht.

2.2 RedTeam is nimmer aansprakelijk voor enige directe dan wel indirecte schade, waaronder gevolgschade, bedrijfsschade, winstderving, schade voortvloeiende uit aanspraken van derden jegens de opdrachtgever, waaronder medewerkers van de opdrachtgever, of welke andere schade dan ook, die in verband staat met de pentest die RedTeam bij de opdrachtgever heeft uitgevoerd dan wel met iedere poging van RedTeam tot het binnendringen van de ICT-systemen en/of computernetwerken van de opdrachtgever. Ook is RedTeam nimmer aansprakelijk voor enige schade die de opdrachtgever lijdt door handelingen die aan derden die RedTeam inschakelt in het kader van de uitoefening van de opdracht zijn toe te rekenen, zoals de leverancier(s) van de rapportagesoftware of de klantportaal applicatie.

2.3 De opdrachtgever vrijwaart RedTeam tegen iedere (verdere) aansprakelijkheid die op RedTeam zou kunnen rusten jegens derden, waaronder medewerkers van opdrachtgever, met betrekking tot de door RedTeam verrichte opdracht. Deze vrijwaring geldt ook voor alle aanspraken die betrekking hebben op schade die zou zijn geleden door een datalek, gegevensdeling en/of het verlies van gegevens die plaatsvind bij derden die RedTeam in het kader van de uitvoering van de opdracht heeft ingeschakeld, zoals de leverancier(s) van de rapportagesoftware of de klantportaal applicatie. Daarnaast vrijwaart de opdrachtgever RedTeam voor eventuele boetes die door de bevoegde autoriteiten, zoals de Autoriteit Persoonsgegevens, kunnen worden opgelegd.

2.4 RedTeam is niet aansprakelijk voor enige schade die de opdrachtgever lijdt doordat gevoelige gegevens (over eventuele kwetsbaarheden) van en/of over de opdrachtgever door een derde worden bemachtigd door bijvoorbeeld een beveiligingsincident dat plaatsvindt bij de leverancier van de rapportage software en/of de klantportaal applicatie, of door het verlies van toegangs- en identificatiecodes tot de klantportaal applicatie door de opdrachtgever zelf. De opdrachtgever zal vertrouwelijk omgaan met de toegangs- en identificatiecodes waarmee hij toegang verkrijgt tot de klantportaal applicatie en zal deze slechts aan geautoriseerde personeelsleden uit de eigen organisatie kenbaar maken. Artikel 7.2 van de algemene voorwaarden van RedTeam Cyber Security B.V. blijft onverkort van toepassing.

2.5 De vrijwaringen als omschreven in dit artikel zien niet op schade die ontstaat door een toerekenbare tekortkoming bij het uitvoeren van de onderhavige opdracht c.q. pentest door RedTeam dan wel bij opzet of bewuste roekeloosheid.

2.6 Artikel 16. van de algemene voorwaarden van RedTeam Cyber Security B.V. blijft onverkort van toepassing.

Artikel 3: Hosting van systemen bij derden

3.1 Mocht het in het kader van de uitvoering van de opdracht nodig zijn dat door derden geleverde diensten, zoals hostingdiensten, SaaS-diensten of Security Operations Center diensten, moeten worden onderzocht, dan zorgt de opdrachtgever vooraf voor schriftelijke toestemming daartoe van die derden.

3.2 De opdrachtgever is verantwoordelijk voor het inlichten van diegene die hinder kunnen ondervinden van de te verrichten opdrachten. Indien van toepassing, zal de opdrachtgever de internetprovider en hosting-organisatie op de hoogte stellen van de te verrichten opdrachten.

Artikel 4: Geheimhouding

4.1 RedTeam en de opdrachtgever dragen er zorg voor dat alle informatie en gegevens die in het kader van de uitvoering van de opdracht tussen RedTeam en de opdrachtgever worden uitgewisseld, waaronder de resultaten uit de pentest, met het hoogst mogelijke niveau van vertrouwelijkheid worden behandeld door beide partijen.

4.2 De verkregen informatie en gegevens zullen alleen gebruikt worden voor het doel waarvoor deze aan de andere partij zijn verstrekt, zoals het uitvoeren van de pentest, het opstellen van de rapportage en het (doen) herstellen van kwetsbaarheden.

4.3 De resultaten van de pentest zal RedTeam alleen aan de opdrachtgever verstrekken. Indien met de opdrachtgever is overeengekomen dat de resultaten ook via de klantportaal applicatie aan opdrachtgever beschikbaar zullen worden gesteld, zal RedTeam de gegevens uit de rapportage ook verwerken in de klantportaal applicatie.

4.4 RedTeam bewaart de resultaten van de pentest maximaal één jaar na het uitvoeren van de pentest en zal deze daarna verwijderen. Het verwijderen van de resultaten door RedTeam zal geen invloed hebben op de resultaten die via de klantportaal applicatie aan de opdrachtgever beschikbaar zijn gesteld. De opdrachtgever is zelf verantwoordelijk voor de eventuele verwijdering van de resultaten van de klantportaal applicatie.

Artikel 5: Duur en beëindiging

5.1 Deze overeenkomst treedt in werking op het moment van ondertekening door alle partijen en duurt voort totdat partijen aan hun, uit de onderhavige overeenkomst voortvloeiende verplichtingen hebben voldaan.

5.2 Beëindiging van deze overeenkomst ontslaat partijen niet van verplichtingen die daaruit naar hun aard doorlopen. Tot deze verplichtingen behoren in ieder geval de verplichtingen met betrekking tot geheimhouding, aansprakelijkheid en vrijwaring.

Op de onderhavige opdracht en deze overeenkomst zijn de algemene voorwaarden van RedTeam Cyber Security B.V. van toepassing. De toepasselijkheid van algemene (inkoop)voorwaarden van opdrachtgever is uitgesloten.

Onderstaande, indien van toepassing, zo volledig mogelijk invullen:

Technisch contactpersoon opdrachtgever: .....

Telefoonnummer contactpersoon: Direct: ..... Algemeen: .....

E-mailadres: .....

Scope algemeen

.....

Termijn

Deze overeenkomst geldt voor de periode van: ..... tot en met .....

Pentest uitvoering

De tests zullen (deels) extern worden uitgevoerd. RedTeam maakt gebruik van onderstaande IP-adressen:

185.89.155.186 | 18.198.87.232 | 185.109.216.197

94.124.124.18 | 94.124.124.25

RedTeam raadt aan om er zorg voor te dragen dat deze IP-adressen op de whitelist staan. Op deze wijze wordt voorkomen dat de IP-adressen van RedTeam tijdens de test worden geblokkeerd.

De derde partij, indien van toepassing (Internetprovider/hosting-organisatie)

Naam organisatie: .....

Adres: .....

.....

Derde partijen provider geïnformeerd: Ja ☐ Nee ☐

Scope

IP-adressen	Url's

Opdrachtnemer:

RedTeam Cyber Security B.V.

Handtekening:

Datum:

Naam:

Functie:

RedTeam Cyber Security B.V.

Opdrachtgever:

All Automation Service B.V.

Handtekening:

Datum:

Naam:

Functie:

RedTeam
CYBER SECURITY
A OneXillium Group Company

026 20 22 028

info@redteam-security.nl

Meander 901, 6825 MH Arnhem

redteam-security.nl

IBAN: NL40 RABO 0316 2294 23

BTW: NL857106375B01

KVK: 67643744