

Vacature Pentester/Ethical hacker (senior)

Ben je altijd op zoek naar onbekende kwetsbaarheden, de meest complexe exploits en ben je expert in het zelf ontwikkelen van exploits en het uitvoeren van pentests?

Houd je ervan om je kennis en kunde over security, red teaming, exploitation en andere security onderwerpen te delen met collega's en zie je het als een uitdaging om collega's mee te nemen in jouw verhaal? Houd je van brainstormen over de verschillende diensten die NFIR aan onze klanten kan bieden? In deze functie zul je technisch uitgedaagd worden om het beste uit ons team te halen en samen met jouw nieuwe collega's de beste pentesten uit te voeren.

NFIR

NFIR is specialist op het gebied van cyber security. Wij helpen organisaties de gevolgschade van een cyber incident te beperken en stellen digitaal forensisch bewijs veilig om de oorzaak van de schade te kunnen achterhalen. Daarnaast kunnen wij met onze diensten helpen bij het vergroten van de weerbaarheid tegen cyber incidenten en ondersteuning bieden bij het verbeteren van de digitale vitale infrastructuur. Onze ervaren medewerkers, die allemaal goedkeuring van de korpschef hebben ontvangen, zijn in staat klanten op een no-nonsense manier te ondersteunen en te adviseren met onze diensten.

Pentesten

Pentesten is voor bedrijven zeer belangrijk, nu bedrijven en organisaties steeds vaker grote hoeveelheden data bezitten. Met de komst van de GDPR is de beveiliging van persoonsgegevens belangrijker dan ooit geworden en is het voor bedrijven een plicht geworden om deze data te beveiligen. Die beveiliging stellen wij maar al te graag op de proef. Samen met andere ethisch hackers/pentesters zal je aan de slag gaan bij verschillende soorten bedrijven en organisaties om zo te onderzoeken welke kwetsbaarheden bij een bedrijf aanwezig zijn.

Niets is hierbij te gek: Van inloopacties, het uitvoeren van red-teaming acties, versturen van (spear-) phishingmails, tot het testen van printers en applicaties en het inbreken op SCADA-systemen, bij NFIR komt het allemaal voorbij!

Als pentester maak je ook onderdeel uit van ons Incident Reponse team.

Functie-eisen

- Opgeven is voor jou geen optie, geen uitdaging is voor jou te groot;
- Creativiteit zit in je genen, als je linksom niet binnenkomt, misschien wel rechtsom;
- Ervaring met Linux, Windows, OS X en mobiele besturingssystemen zoals iOS en Android;
- Je kan zeer goed omgaan met verschillende tools die je werk makkelijker maken, zoals Kali Linux, Nessus, Metasploit;
- Een pro in het uitvoeren van OSINT-onderzoek;
- Flexibel en in staat om open te staan voor nieuwe attack approaches, het leren van nieuwe tools en in staat om feedback van collega's om te zetten in nieuwe energie om de pentesten nog beter te maken;
- Rapportages en adviezen opstellen, om de klant zo goed mogelijk te informeren over de kwetsbaarheden;
- Communicatief ben je zeer vaardig: aan een niet technische klant kun jij precies uitleggen wat er gevonden is en wat de impact ervan is;
- Je bent flexibel, je begrijpt dat incidenten ook buiten werktijd plaatsvinden;
- Certificeringen/opleiding: relevante HBO/WO-opleiding;
- Je hebt een OSCP-certificering (of vergelijkbaar);
- Minimaal 5 jaar relevante werkervaring;
- Minimaal 32 uur per week;
- Gezien de werkzaamheden is een korpschefgoedkeuring noodzakelijk;

(Vervolg op de volgende pagina)

Arbeidsvoorwaarden

NFIR hanteert een marktconform salaris, op basis van opleiding en ervaring. De secundaire arbeidsvoorwaarden zijn daarnaast zeer goed geregeld (leaseauto, telefoon, laptop, pensioen en verscheidene opleidingsmogelijkheden).

Enthousiast geworden over deze vacature? Of heb je vragen en/of opmerkingen? Neem dan contact op met Arwi van der Sluijs (a.vandersluijs@nfir.nl).