

Humankind
T.a.v. Dhr. J. Keulen
Helvoirtseweg 9
5261 CA Vught

Utrecht, 18 oktober 2024

Ref.: EvD 2024/10/Humankind

Onderwerp: Offerte nulmeting en technische analyse

Geachte heer Keulen en mevrouw Peeters, beste John en Mendy,

Op dinsdag 8 oktober 2024 heeft een kennismakingsgesprek plaatsgevonden tussen Humankind en Securesult. Tijdens deze kennismaking hebben wij zowel onze standaard nulmeting en roadmap (mens-proces en techniek) gepresenteerd, alsmede onze visie op het uitvoeren van een technische analyse van de huidige ICT leverancier.

Deze technische analyse is een diepgaander assessment dan in onze standaard nulmeting en roadmap wordt uitgevoerd.

Op basis van het gesprek hebben wij afgesproken een offerte uit te werken voor de volgende onderwerpen:

- 1) Nulmeting en roadmap Mens en Proces (dus geen technische analyse)
- 2) Uitgebreide Technische Analyse

Waarbij de 1^{ste} in 2024 uitgevoerd dient te worden en de 2^{de} deels in 2024 en deels in 2025.

In onderstaand voorstel treft u bovenstaande onderwerpen verder uitgewerkt en toegelicht.

Met vriendelijke groet,

Edward van Deursen

Jesse van Straaten

NULMETING

Intake en planning

De intake vindt plaats op locatie (Vught). De planning wordt afgestemd en de taakverdeling wordt besproken.

Tijdens het project wordt van betrokken rollen/afdelingen een bijdrage verwacht. Met name:

- Management;
- FG;
- HR;
- ICT;
- Administratie;
- Contractmanagement;
- Eventueel leveranciers.

Tijdens de intake wordt gezamenlijk vastgesteld met wie interviews gaan plaatsvinden.

De werkzaamheden worden in overleg ingepland.

Context bepalen met BIA (light)

Tijdens de Business Impact Analyse (BIA) worden de kritieke processen geïdentificeerd, de impact van een onderbreking van deze kritieke processen bepaald, dit omvat de financiële impact, operationele impact, impact op klanten, juridische of regelgevende impact, en impact op de reputatie. De herstellijdooelstellingen (RTO's) en herstelpuntdoelstellingen (RPO's) vastgesteld. Hiernaast wordt de resourcevereisten (zoals personeel, technologie, informatie, etc.) geïdentificeerd. Ook wordt de prioritering voor herstelactiviteiten vastgesteld.

Assessment

Tijdens het assessment (nulmeting) wordt bepaald in welke mate de organisatie voldoet aan de beveiligingsnormen, i.c. wordt onderzocht hoe de huidige situatie (ist) zich verhoudt tot de ISO 27001 (soll) qua opzet, bestaan en werking. De afwijkingen ten opzichte van deze norm wordt in kaart gebracht. Dit assessment wordt uitgevoerd door middel van interviews, een technische analyse en een documentstudie. Hierbij vormt het overzicht van ICT beveiligingstools van de vaste ICT leverancier van Humankind een belangrijke component.

Technische Analyse

De Technische Analyse maakt normaal gesproken onderdeel uit van de nulmeting en wordt nu los aangeboden vanwege een andere scope dan gebruikelijk.

Risico Analyse

Op basis van de inzichten van de BIA, Assessment en de Technische Analyse vindt een risico analyse plaats. Hieruit komt naar voren welke risico's en kwetsbaarheden als eerste aangepakt moeten worden. De resultaten, aanbevelingen en adviezen worden verwerkt in de roadmap.

Roadmap

De roadmap geeft weer hoe Humankind vanuit de ist situatie de soll situatie (ambitie) kan bereiken, c.q. de implementatie van ISO 27001 kan realiseren.

Stappen voor implementatie normen

In de roadmap geven we aan welke normen/processen/werkzaamheden ontbreken en bijgevolg moeten worden geïmplementeerd om de ISO 27001 over de gehele breedte te implementeren.

De volgorde van implementatie die het beste aansluit bij de huidige situatie van Humankind wordt eveneens in de roadmap aangegeven.

Rapportage en presentatie

Wij stemmen tijdens de intake de vorm van de rapportage af op de behoefte om zo maximale waarde te leveren. In de rapportage worden de bevindingen, aanbevelingen en conclusies opgenomen. Tevens wordt in een roadmap aangegeven hoe het vervolg vorm gegeven kan worden.

Wat we opleveren:

- Resultaten BIA, Assessment en Technische Analyse;
- Geïdentificeerde risico's en kwetsbaarheden;
- Roadmap zoals eerder beschreven;

Uitvoering vs Planning

In de periode november/december kunnen wij de nulmeting uitvoeren.

De planning geschiedt altijd in overleg. Bij onvoorziene omstandigheden waarbij vertraging of uitloop wordt verwacht, vindt onderlinge afstemming plaats om de impact te minimaliseren.

Samenstelling team

De senior consultant die de nulmeting zal uitvoeren wordt op voorhand voorgesteld. Een medior consultant zal ondersteunen bij de uitvoering van de werkzaamheden..

TECHNISCHE ANALYSE

Intake en planning

De intake vindt online plaats in MS Teams. De planning wordt afgestemd en de taakverdeling wordt besproken. Het is mogelijk om op basis van de prioriteiten een deel van de analyse in 2024 en een deel in 2025 uit te voeren. Zodat bijvoorbeeld de reeds bekende risico's omtrent de mailserver, eerder in kaart gebracht kunnen worden.

Tijdens het project wordt van betrokken rollen/afdelingen een bijdrage verwacht. Met name:

- CISO;
- ICT;
- Contractmanagement;
- Eventueel leveranciers.

Tijdens de intake wordt gezamenlijk vastgesteld met wie interviews gaan plaatsvinden.

De werkzaamheden worden in overleg ingepland.

Technische Analyse

Scope van deze analyse ligt op de volgende diensten/producten:

- Networks-as-a-Service
- Firewalls-as-a-Service
- WiFi-as-a-Service
- Werkplek-as-a-Service
- E-mail server

Een Red Team test op de SOC dienstverlening is besproken maar nu niet in scope.

Tijdens het gesprek is besproken om te beginnen met de e-mail inrichting omdat hier een hoger risicoprofiel wordt gezien.

De standaard kwetsbaarheidsscan uit de nulmeting is toegevoegd om zo een compleet beeld te krijgen van de risico's.

Rapportage en presentatie

Wij stemmen tijdens de intake de vorm van de rapportage af op de behoefte om zo maximale waarde te leveren. In de rapportage worden de bevindingen, aanbevelingen en conclusies opgenomen.

Wat we opleveren:

- Resultaten van de Technische analyse;
- Geïdentificeerde kwetsbaarheden;

Een inzicht in de mogelijke vervolgstappen wordt gegeven.

Samenstelling team

De senior consultant coördineert werkzaamheden en presenteert de resultaten. De technische analyse wordt door een ethical hacker en/of een security engineer uitgevoerd.

ONS VOORSTEL

Werkzaamheden nulmeting

Hieronder geven we een overzicht van de werkzaamheden en de uren inschatting.

Onderdeel / Werkzaamheden	UREN INSCHATTING		
	Senior Consultant Securesult	Consultant Securesult	Medewerkers Humankind
Kick-off, intake, scope en planning. Samen de uitgangspunten voor het onderzoek bepalen en afkaderen; afstemming te interviewen functionarissen.	2		2
BIA Bepalen van context, bedrijf kritische processen en systemen en volgorde van herstel met hersteltijden.	4		4
ISO 27001 Assessment Op basis van de ISO 27001 bepalen in welke mate hieraan wordt voldaan, o.a. door het afnemen van interviews en documentstudie.	16	12	24
Risico analyse Inventariseren van risico's en opstellen van risicoregister.	10		4
Roadmap Plan van aanpak, kosten, prioritering.	12		8
Rapportage en presentatie Uitwerken van bevindingen en opstellen van de aanbevelingen.	16		2
Totaal	60	12	44

Werkzaamheden Technische Analyse (los)

Hieronder geven we een overzicht van de werkzaamheden en de uren inschatting.

Onderdeel / Werkzaamheden	UREN INSCHATTING		
	Senior Consultant Securesult	Consultant Securesult	Medewerkers Humankind
Kick-off, intake, scope en planning. Samen de uitgangspunten voor het onderzoek bepalen en afkaderen; afstemming te interviewen functionarissen. Afstemming en afspraken maken met leverancier, o.a. vrijwaring.	2		1
Technische Analyse van leveranciersdiensten Technisch assessment van de volgende diensten en producten: <ul style="list-style-type: none"> • Networks-as-a-Service • Firewalls-as-a-Service • WiFi-as-a-Service • Werkplek-as-a-Service • E-mail server • Kwetsbaarheidsscan netwerk 	2	40	2
Rapportage en presentatie Uitwerken van bevindingen en opstellen van de aanbevelingen.	4	16	1
Totaal	8	56	4

Het betreft hier een overzicht van de uren die nodig zijn voor het uitvoeren van een losse Technische Analyse van de leveranciersdiensten.

Wanneer ernstige bevindingen met een hoog risico worden gevonden worden deze direct gemeld bij de CISO en later uitgewerkt in de rapportage.

INVESTERING

Tarieven en voorwaarden

Wij verwachten dat de functionarissen van Humankind zelf de geplande inspanning daadwerkelijk kunnen leveren. Mocht dit een probleem opleveren dan treden wij met u in overleg om de impact hiervan door te spreken.

We bieden deze assessment tegen een vaste prijs aan. Hiermee komen we tot de volgende investering:

Onderdeel	BEDRAG
Nulmeting conform ISO 27001	€ 9.720,00
Technische Analyse leveranciersdiensten	€ 7.280,00

Bedragen zijn de all-in prijs voor de investering betreffende de (externe) uren van Securesult.

Bovengenoemde bedragen zijn exclusief BTW en inclusief reis- en verblijfkosten binnen Nederland. De facturatie geschiedt 50% vooraf en restant na afronding van de opdracht.

Tarieven voor vervolg

Wij hanteren de volgende uurtarieven.

ROL	UURTARIEF (EX. BTW)
Senior Consultant / Project Manager	€ 140,00
Medior Consultant	€ 110,00
Junior Consultant	€ 90,00

Vooraf wordt de inzet afgesproken (aantal uren per week/maand) en de besteedde uren worden op basis van nacalculatie maandelijks gefactureerd.

Bovengenoemde bedragen zijn exclusief BTW en inclusief reis- en verblijfkosten binnen Nederland.

Op deze overeenkomst zijn de voorwaarden van Securesult B.V. van toepassing.

De offerte is geldig tot 17 november 2024. Indien er nog vragen zijn kunt u contact opnemen met Jesse van Straaten via jvstraaten@securesult.nl.

Indien u akkoord gaat met de hierboven beschreven aanbieding, verzoek ik u de kopie van deze offerte te ondertekenen en te retourneren. Ik vertrouw erop u hiermee een passende aanbieding te doen en zie uw reactie met belangstelling tegemoet.

Met vriendelijke groet,
Edward van Deursen

Voor akkoord Securesult:
d.d. 18-10-2024



Securesult B.V.
Edward van Deursen
Directeur

Voor akkoord:
d.d.

Humankind
Naam:
Functie: