Pentesten doe je zo

Een klantperspectief

alliander

$whoami

Robin²

$ su - Robin Visser – Pentestcoordinator

- Technische Kantoor Automatisering en Bedrijfskundige Informatica
- Functioneel- en technisch applicatieconsultant
- Coördinator voor diverse ITIL processen
- Implementaties van technische systemen waaronder een HSM
- Siten van het slimme meter applicatielandschap
- Draagt zorg voor succesvolle uitvoering van penetratietesten binnen Alliander

$ su - Robin Massink – OT security specialist

- Elektrotechniek en embedded systems
- SCADA protocol conformance tester
- ICS security consultant
- Draagt bij aan vulnerability en Threat management betreffende de OT omgeving van Alliander

Alliander in cijfers

Het licht brandt, de huizen zijn warm

Klanten

- Aantal klantaansluitingen: 5,7 miljoen
- Aantal slimme meters in bedrijf: 3,8 miljoen

Netten

- Ruim 41.000 km gasleidingen
- Ruim 90.000 km elektriciteitsnetten
- Beschikbaarheid van energie: 99,99%

Medewerkers

- Aantal medewerkers (in fte): 5.755

Financiële cijfers

- Netto-omzet: € 1,9 miljard
- Resultaat (na belastingen): € 334 miljoen
- Investeringen: € 731 miljoen

3 oktober 2019

Pentesten binnen Alliander

- Pentesten; onze definitie.
- Waarom doen wij aan pentesten?
- En wanneer..?

Complex.. Wat nu?

Onze methode

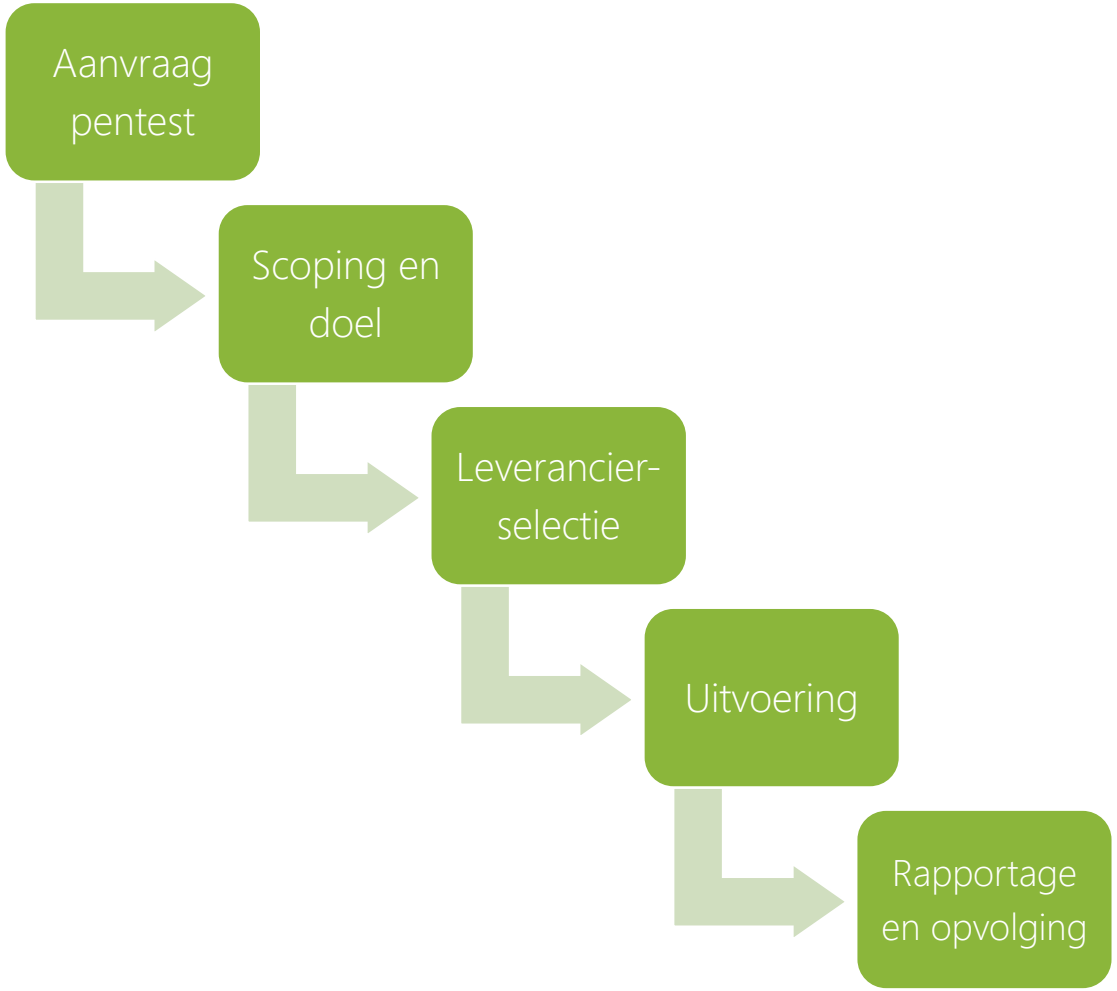
- Wat is het probleem?

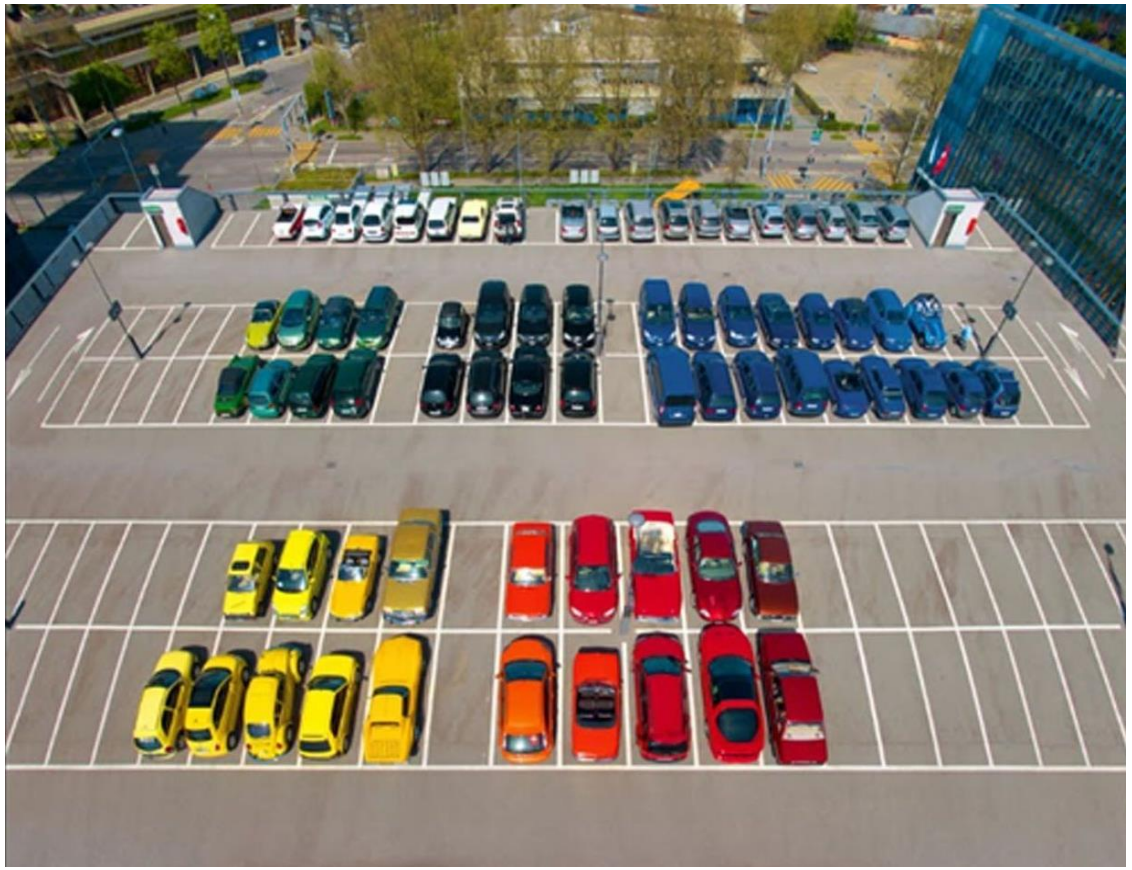
- Oplossing: centrale coördinatie

Centrale pentestcoordinatie

In de praktijk

- Eénduidig proces





Benodigdheden

Templates geven houvast

Logo Leverancier

PCA – Offerte – <<NAAM LEVERANCIER>>

Offertes worden te allen tijde in het Nederlands geschreven tenzij van tevoren anders afgesproken.

Interpretatie Scope

<De beschreven interpretatie van de scope door de leverancier.>

Prijsopbouw en aanpak per opdrachtdeel

Vul hier de aanpak en prijsopbouw in per opdrachtdeel zoals die in de opdracht is aangevraagd.

Opdrachtdeel	Beschrijving van de aanpak	Aantal dagen	Prijs excl. BTW
Deel 1			€
Deel 2			€
Projectmanagement			€
Rapportage			€
	Totaal		€

Planning uitgezet per opdrachtdeel

Vul hier de relatieve planning ten opzichte van de startdatum in per opdrachtdeel zoals die in de opdracht is aangevraagd.

Mogelijke startdatum (o.b.v. aanvraag en beschikbaarheid resources leverancier): ***<datum>***

Week / Opdrachtdeel	1	2	3	4	…	…	…	…
Deel 1	<x>							
Deel 2		<x>						
Oplevering conceptrapport			<x>					

Medewerkers

Naam medewerker	Functietitel	Beschrijf hier de ervaring van de medewerker m.b.t. de scope	Aantal jaar werkzaam voor het bedrijf	Aantal jaar werkzaam in het pentest-vakgebied
[…]				

PCA – Offerteaanvraag

Contactinformatie

	Naam	Email	Telefoonnummer
Alliander Pentest Coördinator			
Interne Aanvrager			
Alliander Inkoop	<in te vullen door Alilander Inkoop>		

Doel van de pentest

<Wat is het doel van deze pentest? Wil je inzicht in het huidige beveiligingsniveau, de mogelijke risico's, etc?>

Functionele beschrijving

<Per onderdeel, waar benodigd wordt geacht, staat hier een functionele beschrijving.>

Te testen securityrisico's

<Is er beeld bij de huidige security risico's op het te pentesten systeem?>

Verwachting van uitkomsten

<Welke en wat voor soort informatie verwacht je minimaal te krijgen om het beschreven doel te bereiken?>

Scope

Één van de belangrijkste onderwerpen bij een pentest is het bepalen van de scope. Wat moet wel meegenomen worden in de pentest en wat niet?

☐Alleen IT ☐Alleen OT ☐Zowel IT als OT

Geef hier per component in de scope een beschrijving. Denk hierbij aan hardware, applicatie, maar ook interfaces:

Opdrachtdeel	#	Scope	Beschrijving van de scope	Voorgestelde soort securitytest
Deel 1				
Deel 2				
Deel 3				

Landschapsplaat

Om een duidelijk overzicht te krijgen van de totale scope is het van belang dat een landschapsplaat beschikbaar in waarin duidelijk alle te pentesten componenten en interfaces in staan. Vermeld ook de nummers uit

Uiterlijke einddatum pentest: *<datum>*
Uiterlijke opleverdatum rapport: *<datum>*

Kunnen de activiteiten binnen kantoortijden (08:00 – 17:00) worden uitgevoerd?
☐ja ☐nee, maar wel op de volgende manier: *<dagen en tijden>*

Planning proces

Verzending RFI:	*<datum>*
Mogelijkheid tot vragenstellen:	*<datum>*
Beantwoording vragen:	*<datum>*
Ontvangst offerte:	*<datum>*
Beoordeling en gunning opdracht:	*<datum>*
Kick-off-sessie:	*<datum> / <locatie>*
Bespreken concept rapportage:	*<datum> / <locatie>*
Voortgangsgesprek:	*<datum> / <locatie>*
Bespreken pre-definitieve rapportage:	*<datum> / <locatie>*

Randvoorwaarden toegang tot systemen in scope

*Om een pentest succesvol uit te kunnen voeren zijn er veelal een aantal zaken die van tevoren worden. Geef hieronder aan welke van deze onderwerpen van toepassing zijn. Onderstaande r moeten door **de aanvrager** geregeld worden.*

Aan de leveranciers wordt gevraagd om te bekijken of hier wellicht nog zaken ontbreken.

Extern	
Er moet een representatieve omgeving beschikbaar zijn.	Ja / Nee
Er moet rekening worden gehouden met de beschikbaarheid en integriteit van de omgeving.	Ja / Nee
Er moeten Alliander-accounts beschikbaar zijn.	Ja / Nee
Er moeten local admin Alliander-accounts beschikbaar zijn.	Ja / Nee
Er moeten Alliander laptops gebruikt worden.	Ja / Nee
Er moet fysieke toegang zijn op een Alliander locatie.	Ja / Nee
Er moet fysieke toegang zijn tot een zone 3 ruimte.	Ja / Nee
Er moeten backups gemaakt worden.	Ja / Nee
Er moet IP whitelisting geregeld worden.	Ja / Nee
Er moeten client certificaten beschikbaar zijn.	Ja / Nee
Er moet 2-factor authentication beschikbaar gesteld worden.	Ja / Nee
Indien gebruik wordt gemaakt van externe diensten in scope, moet er toestemming zijn voor de pentest, namelijk:	<partijen> / n.v
Anders, namelijk:	<anders> / n.v.t
Intern	
Er zijn resources nodig van de volgende IT-teams:	<teams> / n.v.t.
Er moet IT CIB akkoord behaald zijn.	Ja / Nee
Er moet OT CIB akkoord behaald zijn.	Ja / Nee
Er worden mogelijk persoonsgegevens geraakt/gevonden door de	

Practische tips & Tales from the trenches

Voor

- Overtuig van het nut en noodzaak.

Practische tips & Tales from the trenches

Voor

- Faciliteer en maximaliseer de samenwerking.

Practische tips & Tales from the trenches

Voor

- Wat moet een plaats hebben in de aanvraag?

Practische tips & Tales from the trenches

Voor

- En wat moet er juist niet in staan..?

Practische tips & Tales from the trenches

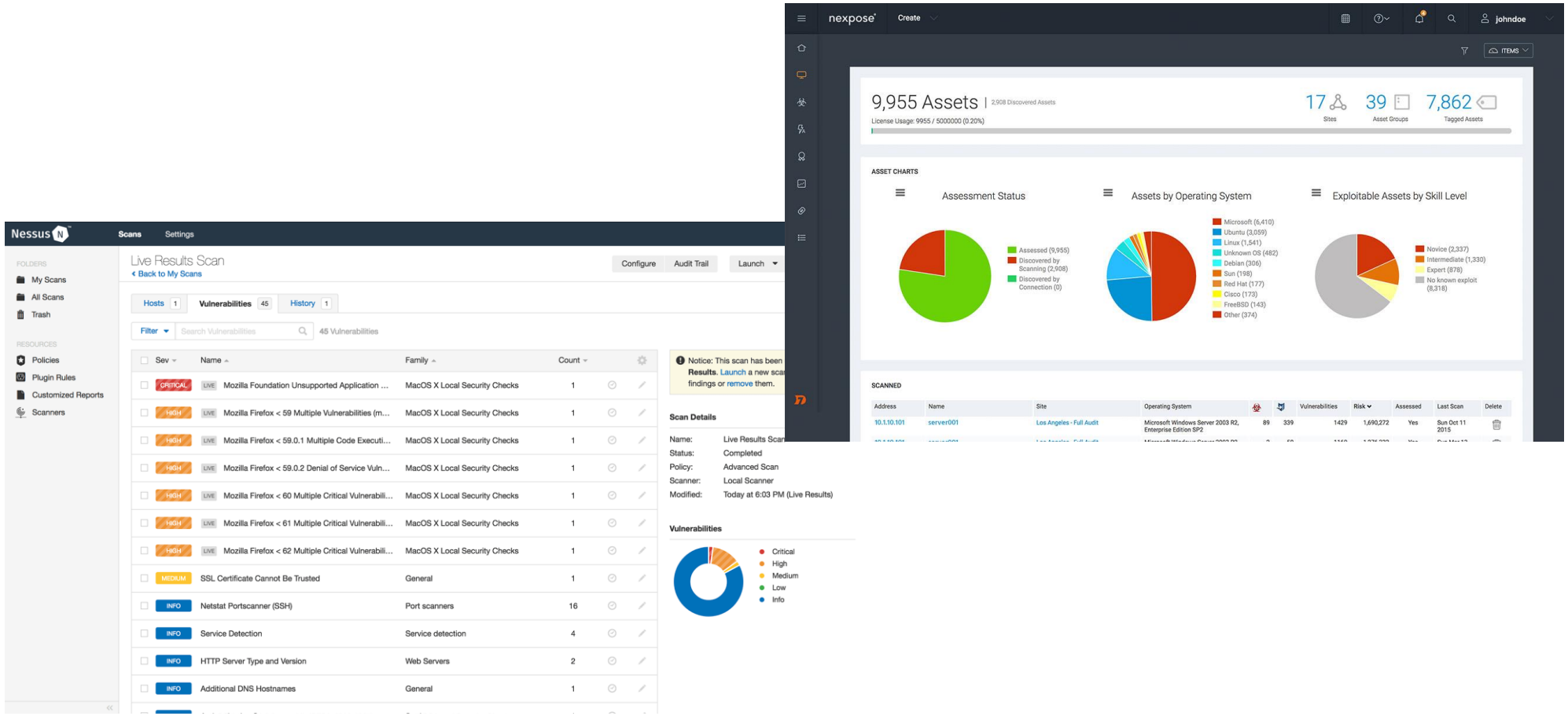
Voor

- Waar ben je naar op zoek? Wat wil je dat de test beantwoord?

Practische tips & Tales from the trenches

Voor

- Kan je niet af met een zelf uitgevoerde scan?



Practische tips & Tales from the trenches

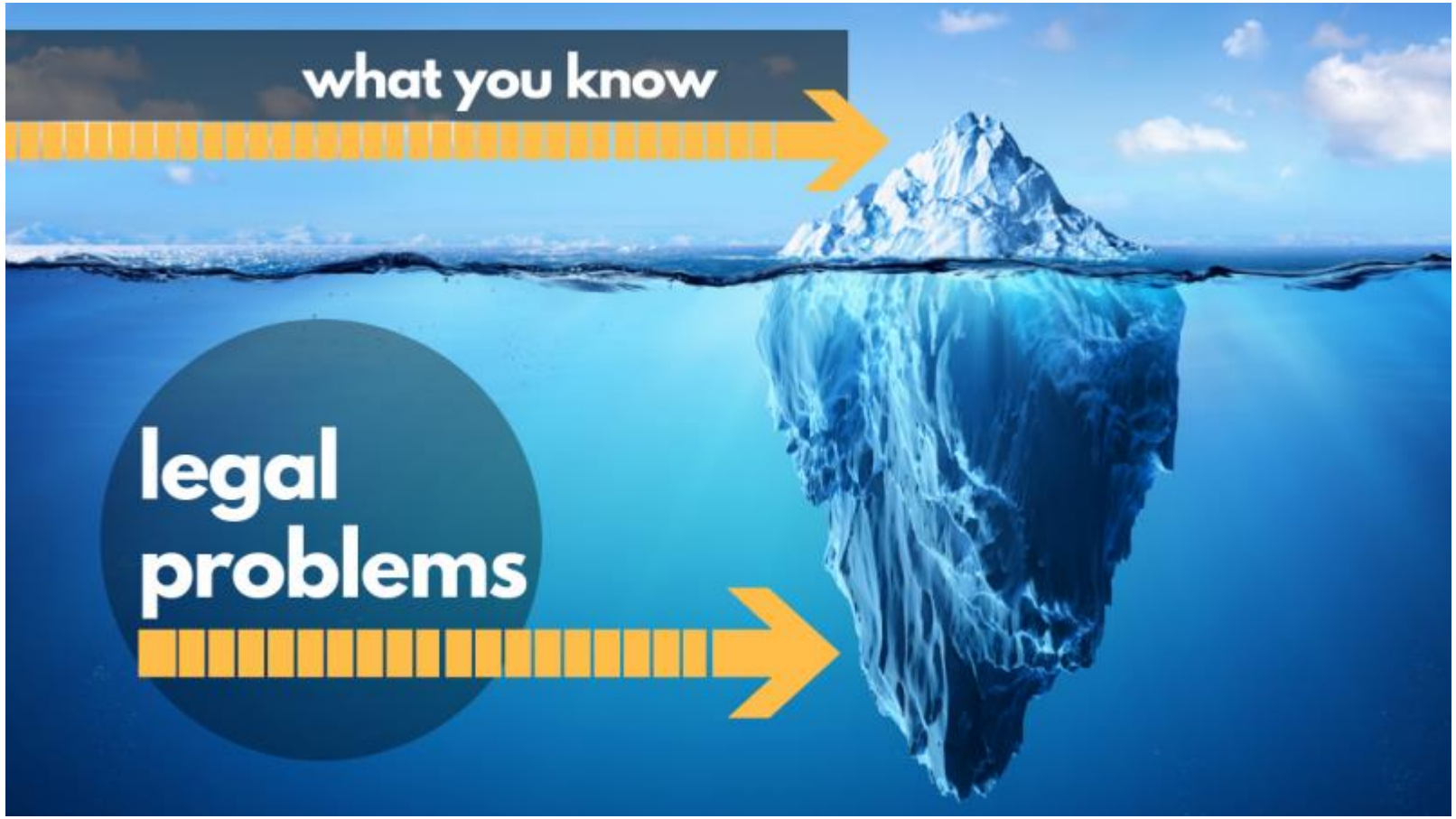
Voor

- Weet je welke partij ervaren/kundig is betreffende de scope?

Practische tips & Tales from the trenches

Voor

- Hoe gun je de opdracht? Wat mag/mag niet?



Practische tips & Tales from the trenches

Voor

- Wie wordt er voorgesteld, en wie komt er daadwerkelijk?

VS

Practische tips & Tales from the trenches

Voor

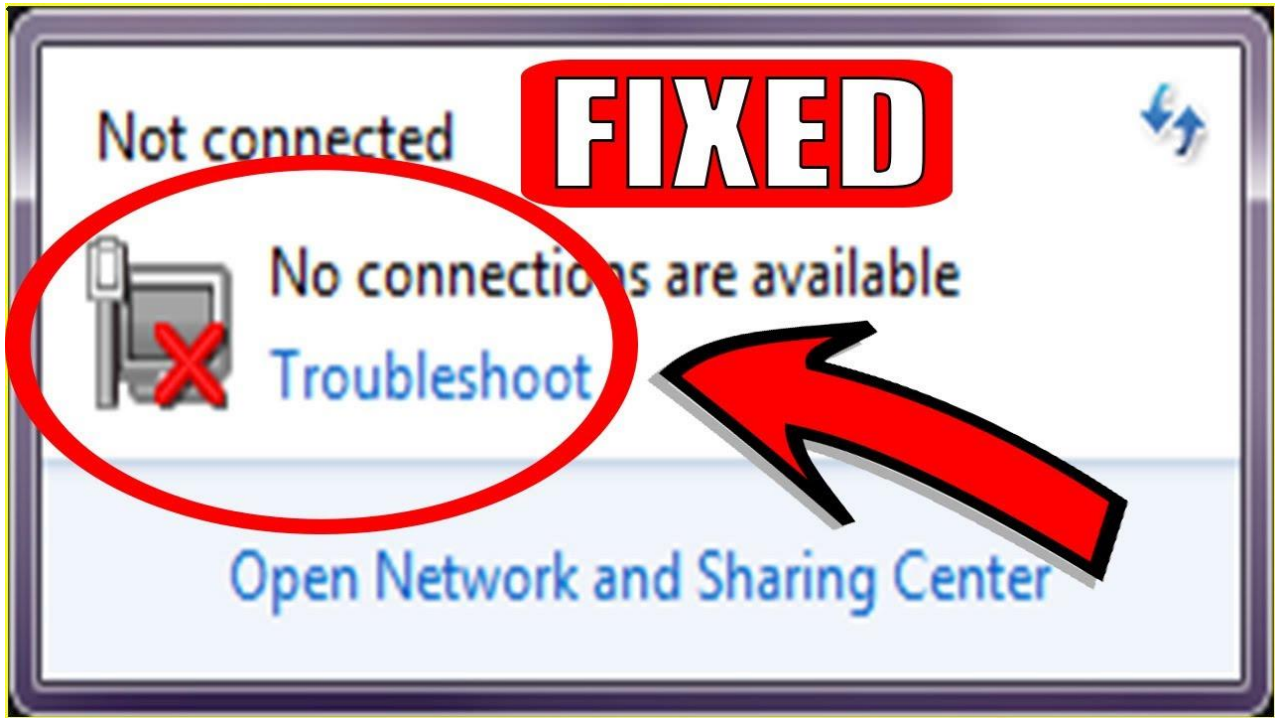
- Beoordelen van offertes, wat is wijsheid?

VS

Practische tips & Tales from the trenches

Voor

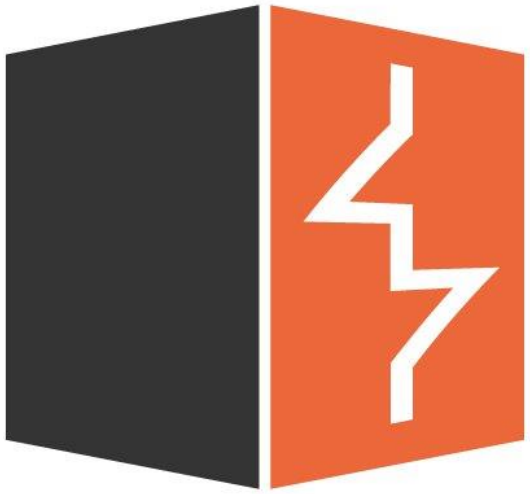
- Welke voorzieningen moeten getroffen worden?



Practische tips & Tales from the trenches

Tijdens

- Met welke tools gaat waar getest worden? En wie levert ze?



Practische tips & Tales from the trenches

Tijdens

- Wie vanuit de organisatie moet geïnformeerd/betrokken worden?

Practische tips & Tales from the trenches

Tijdens

- Wordt er getest op productie of een testomgeving?

Practische tips & Tales from the trenches

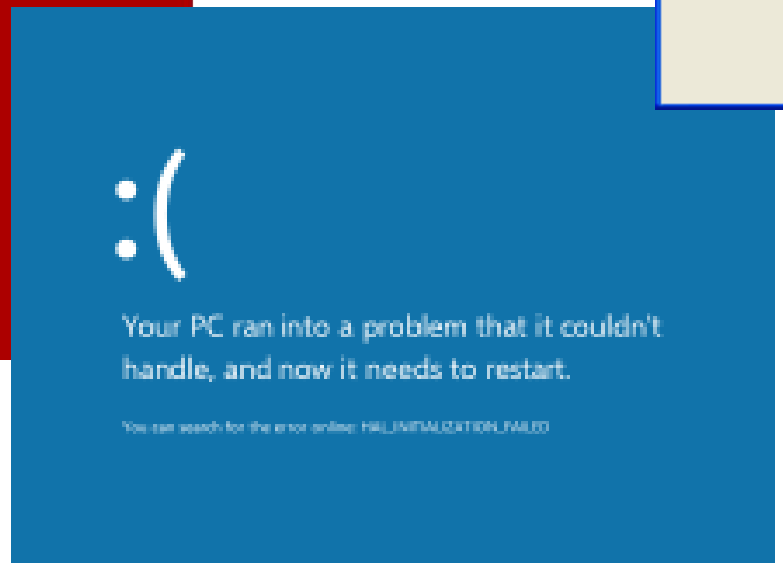
Tijdens

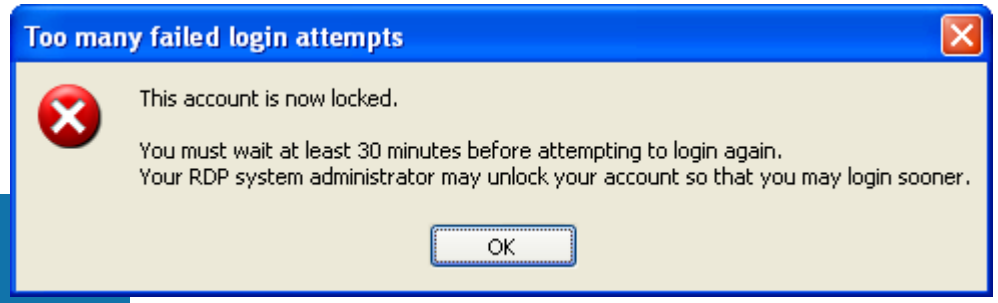
- Kijken de tester naar de juiste zaken?

Practische tips & Tales from the trenches

Tijdens

- Wanneer escaleren we en naar wie?





Practische tips & Tales from the trenches

Na

- Wie mag het rapport hebben?

Practische tips & Tales from the trenches

Na

- Waar mogen resultaten worden opgeslagen?

Practische tips & Tales from the trenches

Na

- Wie mogen de data bewaren?

Practische tips & Tales from the trenches

Na

- Zijn systemen aangetast?

Practische tips & Tales from the trenches

Na

- Zullen we nog even in gesprek gaan?

Practische tips & Tales from the trenches

Na

- Wat gaan we met de resultaten doen?

Vragen?

Contact?

Robin Massink: robin.massink@alliander.com

Robin Visser: robin.visser@alliander.com