R: En nu mijn scherm nu te zien. Klopt dat?
P: Ja.
R: Oké, nou allereerst dank je wel voor het deelnemen aan deze studie. Ik doe onderzoek naar software producten kwaliteit en in het specifiek naar de standaard ISO 25010. ISO 25010 is een internationale standaard die guidelines beschrijft voor het bouwen van goede software producten en dat doen ze aan de hand van kwaliteits karakteristieken. Er zijn acht kwaliteits karakteristieken. Dat zijn functional suitability, performance efficiency, reliability, compatibility, portability, usability, security en dan vergeet ik er even eentje. En in het eerste deel van mijn studie heb ik discussiegroepen gehouden. Dus ik heb bijvoorbeeld ook <naam collega> erbij gehaald. En in die discussiegroepen hebben we voor elk van deze acht karakteristieken gebrainstormd naar objectieve metingen. Dus datapunten die we kunnen meten om iets te zeggen over dit karakteristiek. Daar is een hele lijst van measures uitgekomen. En in dit gedeelte zijn we benieuwd naar waar we deze datapunten mogelijk uit het systeem kunnen halen. Sommigen zullen makkelijker te meten zijn, sommigen zijn misschien moeilijker te meten. En dat is waar we geïnteresseerd in zijn.
Dus in het tweede gedeelte ga ik met, ik heb acht deelnemers in totaal gevonden, dus ik heb met elke deelnemer 1 karakteristiek besproken. Dit is het allerlaatste interview dat ik moet afleggen. En dan gaan we langs de metrics voor één karakteristiek. En de laatste die nog openstaat is security. Goed, ik ben aan de hand van twee dimensies. De difficulty of obtaining data. Die is laag wanneer je de data makkelijk kan verzamelen of makkelijk uit de source kan wegtrekken en het over het algemeen het één uur tot een dag duurt voordat je data beschikbaar kan maken. Dan heb je moderate. Dan is het iets lastiger.
Vaak moet je de data nog iets modificeren of de data moet eerst gecleaned worden voordat je hem kan verzamelen. Dus gemiddeld genomen één dag tot de week. En als de data algemeen unavailable is en je echt een grote effort moet doen in deze available maken, dan hebben we hem ingesteld op meer dan een week. Dan hebben we ook nog de dimensie technische expertise. Die is laag wanneer je eigenlijk alleen maar basic technical skills nodig hebt om te implementeren. Bijvoorbeeld het aflezen van een dashboardje of het bekijken van een waarde in Jira. Dan hebben we moderate. Dat zijn skills die meest software developers wel hebben. Dus het implementeren van een measurement kan door meest software developers gedaan worden. En dit is bijvoorbeeld kennis van een specifieke tool, maar niet in grote mate. En dan hebben we nog high. En dat zijn geavanceerde technische skills, dus in-depth knowledge over een specifieke tool. Is het voor jou duidelijk wat we zo meteen gaan doen? Belangrijk dat je zoveel mogelijk redoneert vanuit je eigen context.
Ik heb eerst een pilot interview gehaald en eigenlijk wilde ik iets zeggen over heel veel software producten in het algemeen, alleen dat is gewoon bijna niet feasible om te doen.
En toen kreeg ik al gelijk feedback van: richt het op een zo specifiek mogelijk context.
Dus waar ik kan, richt het verhaal ook een beetje op jouw context. De eerste vraag om die context verder duidelijk te stellen, is de vraag, wat doe jij bij <naam organisatie> en wat is de tool stack die jullie gebruiken?
P: Ik werk in het data lake. Wij bouwen een data lake als zijnde platform. Het idee is dat federated engineers op ons platform data sets door het data lake heen kunnen trekken.
En wij zijn dan verantwoordelijk voor de functionaliteit van het platform. Zo dat het makkelijk is voor de federated engineers te implementeren.
R: Oké, cool. En wat voor tech stack gebruiken jullie erbij?
P: Je bedoelt CDK of?
R: Exact, ja. Gewoon alle technologieën die gebruikt worden bij het implementeren van...

P: Ja, we werken volledig <inaudible>. Dus in de cloud, AWS, gebruiken we CDK om onze resources te deployen. We gebruiken Python met Spark om onze ETL transformaties te doen. We gebruiken GitHub workflows voor onze pipeline. JFrog voor packaging.
En voor de rest nog niet heel veel tools, maar dingen als Sonar Cloud zijn we wel naar mee aan het kijken. Ja, er is nu nog een beetje een fase waarin we zitten waar die tools nog niet zo ver uitgebouwd zijn.
R: Oké, goed, ik denk dat de context heel duidelijk is. Omdat ik je ken, wist ik natuurlijk deels al alleen ook voor de studie natuurlijk. Oké, wij gaan ons dus richten, dit zijn de andere twee die ik vandaag heb gedaan, op security. Dus hoe het te werk zou gaan, ik noem een bepaalde measure, en dan gaan we sparren over waar zou je dit data punt mogelijk uit kunnen halen. Dus dat kan bijvoorbeeld een code base zijn, dat kan Jira zijn.
Of dan is het Jira of Github Projects, whatever je gebruikt voor project management tool. Kan van alles zijn, het kan bijvoorbeeld een dashboard zijn die ergens ligt. En vervolgens gaan we dus die twee dimensies benaderen. Duidelijk wat de taak is? Oké, de eerste voorgestelde measure die iemand voorstelde was om de veiligheid van een applicatie te meten, kan je gaan tellen voor hoeveel records of hoeveel mensen data verloren is.
Dus de vraag die erbij hoort, dat is eigenlijk de vraag die we dus 19 keer gaan bespreken. Dus ik hoop niet dat het een te saaie sessie wordt. Hoe zouden we dit kunnen meten?
P: In ons geval, wij gebruiken datacontracten om onze distributeurs pas te leggen. Dus die datacontracten die worden gestoord in de repository. Dus als er zo'n growth measure, en die slaan we ook op in de database. Dus die zou je eventueel kunnen queryen. En dan heb je het aantal consumers waarvoor de data verloren is.
R: Hoe weet je dan, hoe kan je zien of er data verloren is? Uberhaupt.
P: In principe zou dat inderdaad eigenlijk nooit de bedoeling moeten zijn
omdat je alles stort in een landing layer. We geven het aan consumers in een distributielayer. Dat is gewoon compleet gescheiden van elkaar. Het kan wel zijn dat de data verloren is tijdens de integratie. Dat is lastig om te detecteren. Het meest voorkomende is dat er op twee verschillende momenten. Dat er gewoon een current state van een source system wordt gestuurd en dat updates die daar tussen hebben plaatsgevonden nooit het data lake bereiken. De manier waarop we dat detecteren is met een intake met het source systeem. Dus daar hebben we ook een contract vast te leggen, wat er precies gebeurt tijdens de integratie. Sommige source systemen zullen niet in staat zijn om al die updates mee te sturen.
R: Dat snap ik inderdaad.
P: Als source hebben we nu de datacontracten die in een repo en in de database staan. In het geval dat je wilt kijken welke data verloren gaat, is het een iets lastiger verhaal om achter te komen.
R: Ik denk dat dat het volgende puntje is, de difficulty of obtaining data. Als je dit getal wilt ophalen. The number of persons for which data is lost. Hoeveel effort zou je daarin moeten stoppen? We kunnen terug gaan naar de scale die erboven staat. Low is dat de data kan binnen een uur tot een dag beschikbaar gemaakt worden. Moderate is misschien een dag tot een week aan effort om de data beschikbaar te maken. En high is het kost je wel meer dan een week om dit getal op te kunnen halen. Om uit te kunnen vinden voor hoeveel mensen, exact ja, data verloren is.
P: Ik denk dat het, als je met een rough measure, als je daarmee oké bent, aantal consumers, dan is het low.

R: Ik denk dat dat inderdaad hier de bedoeling is. We gaan rough measure bekijken en in de toekomstige stap, of in een vervolg onderzoek, kan men verder induiken op bepaalde metrics.
P: Oké, dan is het low. Dan kun je met de middel van een script dat de repository uitlijst, kun je dit allemaal...
R: Check ja, en hoeveel, zeg maar, om die measurement dan vervolgens te implementeren, hoeveel technische expertise zou je nodig hebben? Wederom dus, de skill low, basic technical skills, moderate technical skills nodig. De meeste developers kunnen wel misschien kennis van een tool en dan high in-depth knowledge van een specific tool.
P: Ook low, dat is wat je net beschrijft, een simple script.
R: Oké, duidelijk. Is de vraagstelling voor jou duidelijk en de manier waarop we deze vragen beantwoorden?
P: Ja.
R: Oké, als het op enig punt niet zo is, laat het ook gewoon even weten. Sommige measures zijn natuurlijk vrij vaag en het is juist de bedoeling dat we die dan gaan evalueren.
De volgende measure is het percentage van data dat je geencrypt hebt. Hoe zou je daarachter kunnen komen? We gaan dezelfde stap nu nog 18 keer doen.
P: Oké, AWS heeft een default encryption op alle data. Je kunt ervoor kiezen om zelf of met een KMS key de data te encrypten. Volgens mij doen wij dit op dit moment niet.
R: Oké. Het zelf encrypten?
P: Ja.
R: En stel dat je binnen een platform zou werken waarin data niet geencrypt zou worden. En je wilt wel achter dit nummer komen. Ik weet dat bij jullie het nummer gewoon 100 is in dit geval. Maar stel je zo aan iemand moet aantonen dat het nummer 100 zou zijn. Waar zou je dit nummertje vandaan moeten kunnen halen?
P: Ja, dit is nergens gestoord omdat we de default implementatie. Het is een beetje handwerk, denk ik. Er is geen objectieve measure die ergens staat die we, ja je kunt natuurlijk gewoon met een Boto script al je bucket configuraties uitvragen.
In die zin is het wel de makkelijkste manier. Je source is dan eigenlijk je data. Dus het data encrypted plus een script.
R: Oke, en dan weerom dezelfde twee vragen. Hoe moeilijk zou het zijn om dit te verkrijgen? En hoeveel technische expertise heb je nodig?
P: Low. Alle bucketslisten en vervolgens langs gaan om één.
R: Exact, ja. Easy enough so far. Oké, vervolgens heeft iemand gesteld van dit is puur een boolean value. Een belangrijke waarde om te meten is complyen aan de GDPR. Dus om te complyen aan de GDPR, welke informatie heb je nodig?
P: Deze is misschien iets groter. Wat GDPR is en wat compliant betekent.
Ik denk dat dat het grootste probleem is. Op het moment dat je dat weet, kun je GDPR implementeren. Dit is vooral de right to be forgotten, denk ik. Dat is lastig te meten, want je moet specifieke voorbeelden hebben om te kunnen detecteren of die data daadwerkelijk gedeliet is. En potentieel moet je al je datasets langs, of je moet weten waarin het staat. Dus dit is, ik denk, lastig. Je zult er echt een systeem voor op moeten bouwen, zodat je het efficiënt kunt doen. En op het moment dat dat eenmaal staat, dan is het in feite een query. Dus dan is de technische expectatie niet zo hoog. Maar om het voor elkaar te krijgen, heb je best wel veel kennis nodig.
R: Ja, dus eigenlijk gewoon high high in dit geval.
P: Ja, als je dat maar van de ground-up krijgt. Als je van de ground deze implementatie moet maken en deze measurement moet verzamelen om uiteindelijk te weten, ben je GDPR

compliant? Dan moet je eerst gewoon een complex platform opzetten. En het is lastig om de data nog te verkrijgen.
R: Oké, vervolgens stelde iemand, je telt het aantal security breaches en dat vergelijkt je met een bepaald goal. Want in sommige applicaties is het misschien toegestaan om kleine security breaches te hebben. Misschien als je niet met PII werkt. Dat hangt ook heel erg van je organisatie af. Dit is in ieder geval wat iemand in de focus group stelde. En het gaat dan vooral dus om het tellen van de security breaches. Waar zou je dit nummertje uit kunnen halen?
P: Verschillende dingen. AWS heeft een dashboard waarin je dit soort standaarden, waarin ze een aantal dingen meten. Er zijn tools zoals CDK-nagging, die kan je gebruiken om potentiële security issues te vinden. CDK-nagging is een tool die je gebruikt voor het achterhalen van infrastructuur specifieke. Ja, het heeft bepaalde rules op je CloudFormation template, wat een potentiële security risico is.
R: Dan plak ik die voor alvast hier, want deze komt ook nog. En dan zou je ook security breaches kunnen meten?
P: Ja.
R: Oké. Gezien het een dashboard is, is dit iets wat al readily available is, want dan is het natuurlijk makkelijk. Mag ik om de data te optelen, of moet je hier iets van een custom implementation voor maken?
P: Ja, sommige dingen zijn oké, en het is irritant dat het in je dashboard blijft staan en in je overview. Maar als je alleen geïnteresseerd bent in dit nummertje, kan je die eigenlijk vrij eenvoudig vinden. Het is lastig om dan aan het nummertje een betekenis te koppelen, want je weet niet hoeveel van die dingen oké zijn.
R: Dat is zeg maar oké binnen deze context, want deze measure die kan je dan puur losnemen. En dan, als je hem in combinatie met alle andere measures meet, pas dan geef je de betekenis aan. Dus de studie die claimt ook niet om betekenis aan je measures per se te geven, maar puur getallen die mogelijk interessant zijn.Dus vanuit die context zou het dan eenvoudig zijn, maar wil je echt betekenis aan dat nummer geven, dan is het iets complexer. En dan hang ik natuurlijk weer af van het type breach.
P: Oké, ja.
R: En gezien het puur het aflezen van een dashboard is, stel, zou ik ook stellen dat er weinig technische expertise voor nodig is?
P: Ja.
R: Oké, laten we doorgaan naar de volgende. So far so good, vraagstelling duidelijk wat we aan het doen zijn. Verder een remark?
P: Ja, één onduidelijk ding. Wat als, oké, de nummer of security breaches, je meet misschien niet alles. Dus er zit wel bijvoorbeeld een onzekerheid in het dashboard wat je hebt.
R: Klopt, klopt. Ja, dat is iets waar je eigenlijk niet zoveel aan kan doen.
Dus inderdaad, misschien om de measure verder aan te scherpen, ik heb ze nu gewoon overgenomen zoals ze zijn genoemd tijdens de focus groups. Zou de measure moeten zijn number of known security breaches, want degene die je niet weet kan je ook niet echt meten op een manier.
P: Ja precies.
R: Ja, maar goede remark inderdaad wel bij. Oké, de volgende focus group die stelde je kan security meten door het aantal mensen met production access te tellen. En dat te tellen met, dat te delen door het totaal aantal mensen met access.

Waarin zij steldne, of je het ermee eens bent of niet, dat is niet wat we hier hebben bespreken. Dat zo min mogelijk mensen access tot prod zouden moeten hebben.
P: Ja, in eerdere situaties komen we dat in de account gewoon zien, maar in de huidige account hebben we geen users. Iedereen maakt gebruik van role. Dus dan moeten we het zien in de repository wie er access heeft om. Eigenlijk wie er, nee, ik zeg eigenlijk verkeerd. Iedereen die een bepaalde rol kan assume, die heeft read access in prod. En eigenlijk zijn er maar twee personen die elevated privileges hebben in onze productie account.
Dus dat is gewoon tech lead in de architect.
R: Dus nieuw is eigenlijk people who can assume role plus elevated privileges. En hoe weet je welke mensen die rol kunnen assume?
P: <naam team> houdt dat denk ik in de gaten, want die request maak je bij hun. Ja, exact.
R: Ja, dus dit is niet data waar jullie zelf over beschikken, maar hier is een dependency op een ander team om deze data te geven. Mocht je iets willen zeggen over deze metric.
P: Ja, roles plus elev.
R: Oké, en om dit getal te achterhalen, hoe lastig zou dat zijn?
P: Moderate. Het is een external team, dus daar zit altijd een delay tussen.
R: Exact, ja.
P: Technical expertise, low. Iedereen kan een e-mail schrijven.
R: Oké, nu hebben we een tweetal die gaat over het aantal open security issues.
En het eerste is dat je per severity code bijhoudt hoeveel open security issues er zijn.
Waar kun je deze informatie vinden? Dat is dan weer een ondervraag. En dan hebben we het eigenlijk weer over de security issues uit twee measures geleden.
P: Ja, exact, ja.
R: Alleen dan nog specifiek per severity code.
P: Ja, in principe ook gewoon in het dashboard en in de error message die je krijgt bij een nagging. Daar staat, dacht ik, de security code bij. We gaan er wel van uit, dat is logisch.
R: Oké, makes sense. Gezien je dan dezelfde source gebruikt, zou je stellen dat de difficulty obtaining data en technical expertise wederom gewoon hetzelfde is?
P: Ja.
R: Oké, vervolgens hebben we de open security issues voor infrastructure. En eerder noemde je al cdk-nagging. Dus ik neem aan dat we deze al hebben ingevuld eigenlijk.
P: Ja.
R: Goed, ook deze heeft overlap met wat we eerder hebben gehad. Dus the number of people with admin privilege. Dus wederom, is het ook iets wat in <naam team>?
P: In de account, ja. In de repository zijn er meer mensen. Daar is het iedereen van ons eigen team. En daar verder weten de engineers, zijn er geen admins. Dus de source is dan ook in GitHub.
R: Waar zouden ze informatie vervolgens dan kunnen vinden?
P: In GitHub, wie er in ons team zit. Ja, maintainers. Oké, en dit is puur het bekijken van de GitHub repository, right?
R: Oké, easy enough. We lopen er goed doorheen. Oké, vervolgens is de measure a number of times break the glass activated. Dus hoe vaak moet je gebruik maken, hoe vaak kom je in een situatie dat je gebruik moet maken van elevated privileges?
P: Relatief vaak, omdat het zo werkt dat we helemaal niks kunnen aanpassen. Dat we helemaal nul right access hebben in acceptance en productie.
R: Dus bij jullie zou dit nummer vrij hoog zitten, dus?
P: Ja.

R: Oké, en om achter dit nummer te komen, hoe zouden we dat kunnen meten? Wordt dat ergens bijgehouden, hoe vaak het wordt gedaan? Of kan je dat ergens bijhouden?
P: Ja, <naam team> houdt bij hoe vaak die rol wordt geassumed.
R: Ja, wederom een extern team, dus? Wie dat doet.
P: Weet je hoe <naam team> en hoe die LPE accounts werken?
R: Nee, niet precies.
P: Ja, zij providen ons met de account. Wij hebben al onze platform bovenop hun platform. Dus zij bepalen wat je kunt doen, wat voor permission boundary je hebt. En ze configuren wat dingen voor deployment, et cetera.
R: En kunnen we ook een educated guess maken over hoe zij achter dit nummer kunnen komen? Of het voor hen makkelijk zou zijn om te doen? Anders moeten we deze denk ik onder not applicable zetten, omdat wij dit niet doen, maar een extern team.
P: Ik vermoed dat dit volledig geautomatiseerd is. Ik weet het wel, als je dat te vaak gebruikt, dan gaan ze ook wel met je in gesprek. Dus ik vermoed dat ze wel warnings hebben over wat je precies doet.
R: Maar we hebben eigenlijk geen idee in hoeverre en hoe moeilijk dat was om te bouwen, right?
P: Nee.
R: Dus kunnen we deze dan het best onder not applicable zetten, omdat dit weten we gewoon niet?
P: Ja.
R: Geldt hetzelfde dan voor de volgende measure. Dus de number of sensitive request usage actions. En de vorige was hoe vaak worden die elevator purchase gebruikt. Dus hoe vaak wordt die geassumed. En deze is hoeveel acties worden er gedaan met de elevator purchase. Nog een niveau van granulariteit lager.
P: Meten, dat weet ik dus ook niet. Ik heb een rough idee, omdat ik weet wat er mee gedaan wordt.
R: Ja, we kunnen natuurlijk een guess maken. Alleen als het nu een guesswerk is.
Daar zijn we niet echt in geïnteresseerd.
P: Exact, ja.
R: Vervolgens stelden mensen, je checkt puur of de security layer single sign-on used aanwezig is. Hoe weet je of single sign-on aanwezig is?
P: Ook dit wordt door LPE en <naam team> geregeld. En ik heb gewoon een portal waarmee ik in online accounts kan.
R: Ja, dus eigenlijk hier is gewoon als jij nu de kwaliteit van een van jouw producten gaat bekijken. En je gaat deze lijst aflopen. En je zou moeten aantonen dat SSO gebruikt wordt. Dan kan je gewoon naar de portal gaan.
P: Ja.
R: Oké. En aangezien het gewoon een simple click is, is het dan correct om het met low in te vullen?
P: Ja.
R: Nu hebben we weer een aantal die misschien niet applicable zijn. Maar daar kunnen we natuurlijk over discussiëren. We hebben het number of illegal users. Dus hoeveel gebruikers zijn er die misschien niet meer bij de organisatie werken. Of die eigenlijk geen toegang zouden moeten hebben? Is het iets wat jij ook zou kunnen tellen?
P: Nee, onze eigen productie account niet. In de oude productie account, waar we onze eigen users hebben. Daar gaan we nog wel ieder kwartaal alle users langs. En mensen die

je niet kennen. Dan is het echt gewoon handmatig checken of ze een <naam organisatie>-email-adres hebben. En een beetje LinkedIn zoeken als ze nog bij ons werken.
R: Ja, exact.
P: Hierbij zou het mogelijk in het AWS-account plus. Ja, wat kunnen we dan bij zeggen? Ja, gewoon de users in de AWS-account die lopen langs. En dat is relatief lastig.
Het zit ergens tussen medium en high in. En hoeveel technische expertise zou je nodig hebben om dit protocol te volgen? Low, iedereen kan dat.
R: Makes sense. Assume diezelfde situatie, dat je het aantal users kunt bekijken. En je wilt tellen hoeveel users er niet in een groep zitten.
P: Dat zou ik ook weer met een boto script doen.
R: Dus dat is.
P: Allebei low?
R: Check. Oké, dan hebben er nog. Dan komen we nog uit met de tijd.1, 2, 3, 4, 5, 6.
Dan komen we zeker makkelijk uit met de tijd. Hier zegt iemand de hoeveelheid.
Iemand heeft gesteld dat als je meer verschillende security protocollen in combinatie met elkaar gebruikt, of security best practices, encryption bijvoorbeeld, dan is je applicatie beter beveiligd.Hoe zou je dit aantal kunnen tellen?
P: De hoeveelheid protocolen dat je gebruikt? Ik heb geen idee.
R: te specifieke dingen misschien voor jouw scope.
P: Ik denk niet in protocolen en zo, dat is niet de taal.
R: Dan zetten we deze gewoon onder non-applicable. De volgende is het aantal security layers.En met een security layer bedoeld men hier toegangspatronen. Dus bijvoorbeeld als je MFA hebt, dan zou het over het algemeen twee zijn. Een password en dan vervolgens nog een MFA check. Dus hoeveel lagen zitten er tussen? Hoeveel lagen aan beveiliging zitten er tussen?
P: Allereerst, je moet je in je laptop inloggen. Dan heb je je PIN. Dan is het je single sign-on. Dat is eigenlijk in de account.
R: Wat zou de source dan kunnen zijn? Hoe kunnen we deze
een niveau abstracte omhoog trekken?
P: De source hiervan ligt dan ook weer buiten mijn team, omdat ik niet verantwoordelijk ben voor de hardware. En voor de single sign-on.Wederom hier gewoon non-applicable.
R: Dat had ik inderdaad ook al verwacht. De volgende stelt van, op zichzelf
is het niet heel zinvol om te meten, maar in combinatie met alle anderen wel. Je loopt meer risico voor security als je applicatie exposed is met het internet. En dan wederom om aan te tonen, is je applicatie ge-exposed met het internet. Wat kunnen we als source gebruiken?
P: Het datacontract. Daarin staat de integratie beschreven. Er zijn integration patterns.
Iets wat vrij over het internet gaat, neem aan dat dat niet een approved integration pattern is. In datacontract staat de integration pattern. De integration pattern zelf, wat het precies is, staat beschreven op Confluence. Dus het is een combinatie van die twee.
R: Oké. En gezien het puur het aflezen van een waarde op Confluence is, lijkt dit me niet de meest lastige waarde om af te lezen, right? Heb ik daar gelijk in?
P: Ja, maar al de technical expertise is misschien medium om de kennis die je ervoor moet hebben om internet exposure te begrijpen.Ja, begrijpen welke integration patterns
resulten in internet exposure. Ja.
R: Oké, makes sense. Thanks voor de verbetering. De laatste drie, de hoeveelheid data breaches gedeeld door the number of attacks, waarin iemand stelde van, in principe als je

een data breach hebt, er is een verschil. Je kan één data breach hebben voor 200.000 attacks of je kan één data breach hebben terwijl je maar twee keer geattacked bent. Dat is natuurlijk een heel groot verschil. Waardoor numbers misschien, als je die los van elkaar meet, niet zo zijn zoals niet eigenlijk iets over je security zeggen. Dus hoe zouden we deze combinatie kunnen meten? Wat voor, hoe kunnen we dit nummertje achterhalen? Nou, de data breaches hebben we eerst en dan hebben we de hoeveelheid attacks. Hoe kun je zien dat je data gebreached is? En dat je geattacked bent.
P: Ja, dat is geen idee. Je kunt kijken hoe vaak je bitcoins heb moeten betalen. Ja. Als dat vaker dan 0 is, dan is het niet goed. Anders kom je daar niet aan. Geen idee, hierin is gewoon te security specific.
R: Vervolgens hebben we de lines of defense, waarin iemand stelde je kan in je code ook gewoon allemaal mechanismes implementeren, waardoor je minder likely bent om een breach te krijgen. En hoe meer van deze regels je hebt, dat zou wel mogelijk iets kunnen zeggen over hoe veilig je applicatie is. Heeft iemand gesteld. Dus het tellen van deze security mechanism lines. Dus dan gaat het specifiek over hoe je die nog steeds over internet exposure of? Het gaat dus over je code. Van hoeveel regels heb je in je code opgenomen waarin je probeert security related risks te mitigate?
P: Allereerst hebben we gewoon de account zelf, waarin we een aantal dingen gewoon niet mogen, wat door security gemanaged wordt. In onze code hebben we bijvoorbeeld nagging, wat we gebruiken.
R: Hoe zou je deze aantal lines makkelijk kunnen tellen? Is dat überhaupt te doen?
P: Oh, het aantal lijnen code? Oké, nagging, dat is afhankelijk van hoeveel dingen je oké mee bent, omdat je dan een *inaudible* erin zet. Maar gewoon het applying van nagging, dat is een import en het applying op een stack, twee regels per stack. Het meten is lastig, maar je kunt het weten. Je kan in ieder geval je codebase dan dus gebruiken, want in je codebase kan je dus zien van waar die imports bijvoorbeeld zijn gemaakt. Maar het weten is dus wel lastig om te doen. Ja, dat is high effort, want het wordt niet ergens opgeslagen of zo. Het is niet een metric die we verzamelen.
R: En stel dat je dit toch wel wilt doen, dat iemand hierna vraagt, hoeveel technische expertise zou nodig zijn om dit te kunnen doen?
P: Naarmate je meer technical expertise hebt, zul je ook meer van dit soort dingen in je code stoppen, dus er is een self-enforcing circle hier. Maar ook om ze te kunnen identificeren heb je dan technische expertise nodig? Ik zou zeker moderate technical expertise zetten, want je moet ervan af weten en je moet weten hoe je het kunt implementeren, voordat je überhaupt dingen hebt die je kunt meten.
R: En dan hebben we de allerlaatste, dat is number of points of failure. En ik denk dat ze hier eigenlijk eerder number of points of entry mee bedoelden. Dus op hoeveel verschillende manieren zou je mogelijk kunnen het toegaan kunnen krijgen tot jouw systeem? Op hoeveel punten, op hoeveel vlakken moet je je systeem beschermen, omdat er gewoon een entry point in je applicatie zit? Is er iets wat te tellen is?
P: Ja, dat is wel te tellen. Je zou meerdere bronnen met elkaar moeten combineren. Dus je hebt bijvoorbeeld alle integratie mechanismen. Je hebt de mensen die in de account kunnen, die een rol kunnen assumen. Je hebt ambiguity, omdat de external sources zijn en je geen idee hebt hoeveel personen, hoeveel entities toegang hebben tot het entry point dat jij aan je external source geeft. Hoewel dat meestal wel resources zijn, dus dat kan iedereen eens noemen. Het is voor een gedeelte te meten, het is ook voor een gedeelte nooit zeker weten, dus het is best wel

moeilijk om de metric te meten. Je kan misschien de number of known points wel weten, maar de unknown points eigenlijk niet.
R: En dan die number of known points, uit welke sources kan je die dan halen?
P: Weer uit het datacontractwaarin het beschreven staat. Ook uit de code zelf, waarin de permissions worden gegeven, en external sources,zoals CCB, die die request behouden.
R: En dan voor de allerlaatste keer, de difficulty obtaining data en de technical expertise. Dus om deze data uit die sources te extracten.
P: Het is lastig om programmatisch alle permissions uit je code te zoeken.
Misschien wel mogelijk, maar dan is het nog steeds veel effort. Technical expertise, moderate, je moet misschien begrijpen of iets een entry point is of niet. Dus je moet wel wat weten over de code base en over de tool stack die gebruikt is, alleen je hebt niet in-depth knowledge nodig om dat te kunnen identificeren. Ja, je moet onderscheid kunnen maken tussen dingen die je grant aan een resource in onze account
en dingen die je aan external resources kent.
R: En dan vervolgens de difficulty of obtaining the data?
P: Ja, die zou ik wel op high zetten, gewoon veel effort.
R: Oké, thanks, dan hebben we hier onze totale lijst. Ik denk dat we uiteindelijk toch nog best wel veel hebben kunnen invullen. Voor wat we hebben. Alright, super bedankt, dan sluit ik in ieder geval de recording af.