Disconnect in Agile methoden

13 november 2018

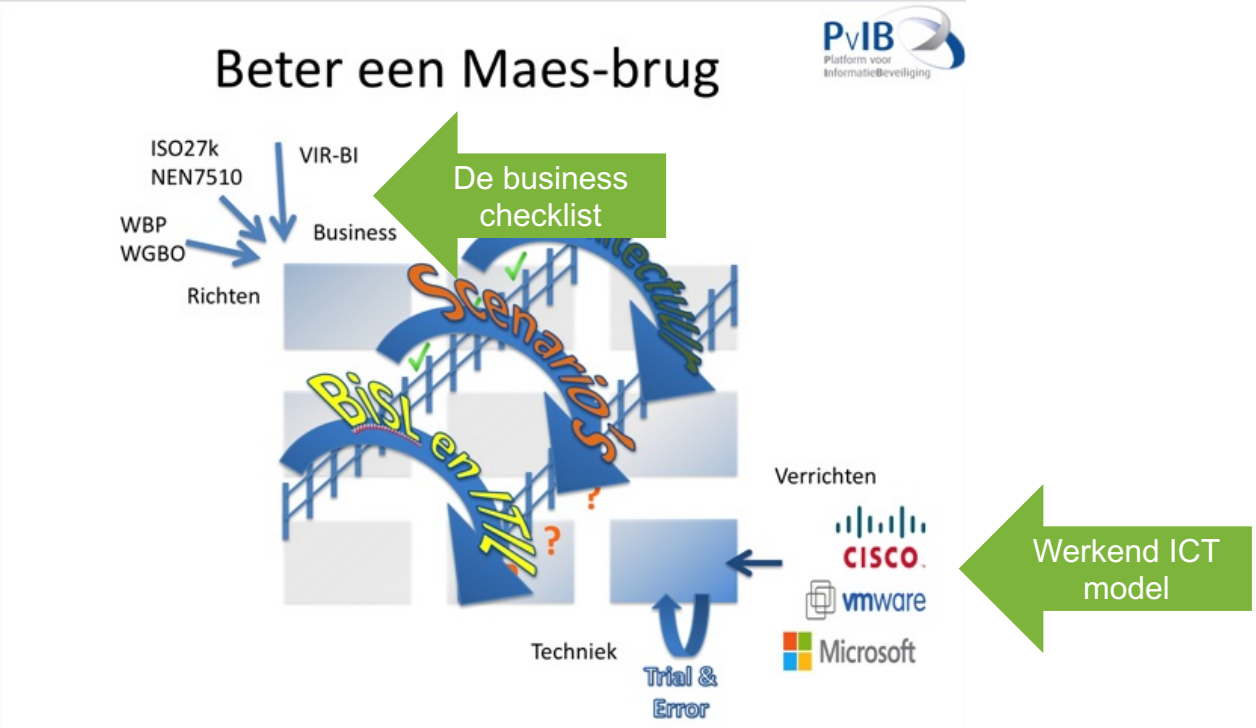
Disconnect in Agile methoden

Whoami

- Riccardo Oosterbaan
- Zelfstandig Architect in (Cyber) Security
  - Nu: Senior Security Architect Alliander
  - Projectleider AVG Aegon
  - API Security Blokker

Thema

- Een belangrijk probleem in informatiebeveiliging is de ‘disconnect’ tussen business en IT. Business weet niet wat ze van de informatievoorziening wil (dat het werkt?) en IT doet dus maar dingen naar beste eer en geweten.
- A. Beerten (2014) bruggen van 1-bureaucratie, 2-verhalen en 3-architectuur.



Model benadering

- Als de regels en het doel precies bekend zijn en er geen onvoorspelbaarheid is dan is een vastgesteld procesmatig model sneller
- Successen behaald op basis van een model zijn voornamelijk in domeinen die veel beperkter zijn dan de echte wereld
  - Welke informatie is in een gegeven situatie relevant (frame probleem)?
  - De dagelijkse realiteit is complex, maar gelukkig er is weer een nieuw managementmodel. Net als alle andere keren wordt succes toebedacht aan dit model
    - Wie heeft er ooit modelvalidatie gedaan op de methodieken?
    - Veelal ontbreken in het model factoren uit de psychologie, cognitiewetenschappen en filosofie
    - Er zijn in de bedrijfsvoering meerdere modellen tegelijkertijd actief
    - Modellen varieren in de tijd
- Hip en Hot: Agile

Agile!

PvIB
Platform voor
InformatieBeveiliging

- Een antwoord op de niet flexibele processen , zoals de watervalmethode. Het
  vorige methodologieën was dat het bouwen van toepassingen zo lang duurd
  vereisten al gewijzigd waren vooraleer het ontwikkeld was. Dit resulteerde in o
  toepassingen.

RAD

- In de traditionele benadering van systeemontwikkeling staan de specificaties vast en moeten deze gerealiseerd worden. Tijd en resources variëren tijdens de ontwikkeling. Een methode die de ontwikkeling van IT-systemen vastlegt in een raamwerk van een tijdsplanning (timeboxes). De duur van het project en de te gebruiken resources worden vast
  project kunnen variëren. In het begin van het project worden op globaal nive
  functionele als de niet-functionele specificaties ingedeeld op prioriteiten (MoS
  de ontwikkeling komen steeds meer gedetailleerde specificaties boven water. De
  gedetailleerde specificaties worden vervolgens ook weer op basis van prioriteiten ingedeeld. Binnen deze tijdsplanning (timeboxes) worden in nauwe samenwerking met de klant eerst de zaken opgeleverd, die het belangrijkst zijn voor de bedrijfsbehoeften van de klant.

D-SDM

Agile!

PvIB
Platform voor
InformatieBeveiliging

- The method defines a set of best practices for application development in optimal conditions by placing the customer at the centre of the development process, maintaining a close relationship with the customer. Based on the following concepts:
  - Development teams work directly with the customer in very short cycles of one to two weeks maximum.
  - Delivery of versions of the software occurs very early and at rapid intervals to maximize the impact of user feedback.
  - There is tight collaboration in the development team when working on the code.
  - The code is tested and cleaned up throughout the development process.
  - Indicators measure the progress of the project so that the development plan can be updated.

Agilissomo!

PvIB
Platform voor
InformatieBeveiliging

- DevOps (een samentrekking van "development" en "operations") is een gebruik[t] een praktijk binnen software engineering die tot doel heeft softwareontwikkeling (D[ev] softwareoperaties (Ops) samen te brengen. Het hoofdkenmerk van de Dev[Ops] het benadrukken van automatisering en monitoring in alle onderdelen bij het b[ouw] software, van integratie, testen, release tot deployment en infrastructuurmanagem[ent]. DevOps probeert te komen tot kortere ontwikkelcycli, een verhoogde frequentie van oplevering en een meer betrouwbare oplevering, in nauwe overeenstemming met de businessdoelstellingen.

Product Owner = head of architecture & security?

- Agile is sterk in opkomst en bijna alle grote bedrijven hebben het inmiddels omarmd voor software ontwikkeling. Daarbij kenmerkt Agile zich door een **sterke focus op persoonlijke interactie** boven traditionele beheersinstrumenten als processen en documenteren.

Psychologie, cognitie en filosofie?

Waar is de disconnect?

PvIB
Platform voor InformatieBeveiliging

- Spanningsveld tussen Short term Business opportunity en mid-term risk
  - Minimum Viable product (een product met juist genoeg functies om eerste gebruikers tevreden te stellen en feedback op te halen)
  - Contracten, Architectuur Design en security. (Time to market: If you cannot beat them diffuse them!)
- Bias in het D-SDM model is als volgt:
  - Focus on the business need => Minimum Viable Product!
  - Deliver on time => Time to market!
  - Collaborate
  - Develop iteratively
  - Communicate continuously and clearly
  - Demonstrate control
  - Never compromise quality => Minimum Viable Product?
  - Build incrementally from firm foundations => Time to market?

Waar is de disconnect?

PvIB
Platform voor InformatieBeveiliging

- Bias in het Devops model met de omgeving is als volgt:
  - Customer collaboration over contract negotiation
    - Het mijden van requirements die niet bijdragen aan snelheid van ontwikkelen van functionaliteiten
  - Working software over comprehensive documentation
    - Dus wacht even, ik heb moeite om resultaat te boeken, de programmeurs willen liever niet teveel tijd kwijt zijn aan documentatie, dus ...
    - Security designs kunnen complex zijn en vergen uitgebreide designs
  - Responding to change over following a plan
    - Jaarplan, afdelingsbudget. Door management opgelegde Unit KPI's
  - Individuals and interactions over processes and tools
    - Scarce Developers are drawn to simplicity and want to minimize the perceived burden of security. Rest/Json populairder omdat SOAP/XML moeilijker te programmeren is.
- Voorbeeld: Faulty reward functions door ontbreken cognitie. We gaan met elkaar sportief racen
  - https://youtu.be/tlOIHko8ySg

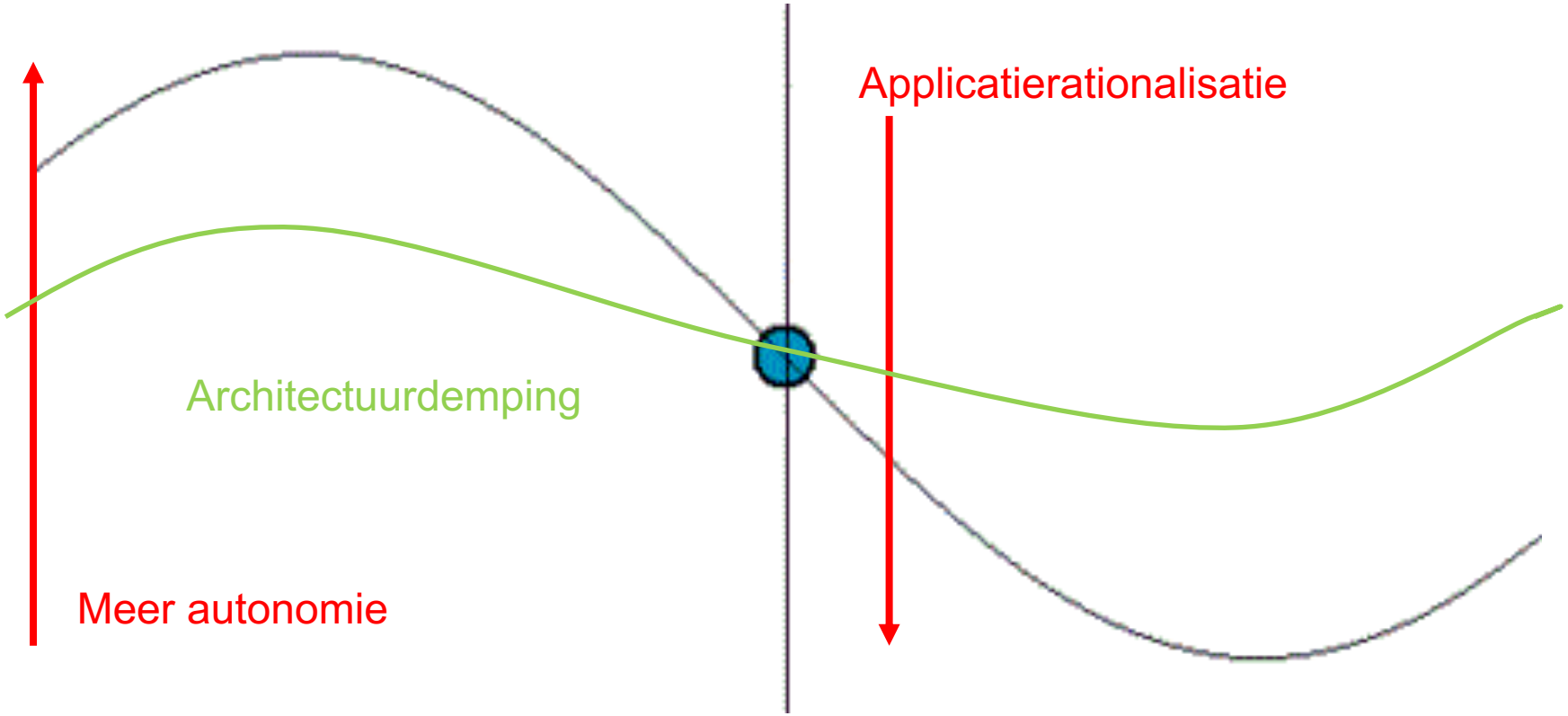
Disconnect in tijd

PvIB
Platform voor
InformatieBeveiliging

- Spanningsveld tussen Autonomie en Enterprise Architectuur (golfbeweging)
  - Strakke (Togafachtige) discipline. Enterprise architectuur maakt i.c.m. het management een charter voor 4 jaar en alle projecten vloeien daaruit voort.
  - Projectleiders worden qua inhoud aangestuurd door EA en het charter.
  - Bijeffect van de Agile gedachte:
    - We hebben geen EA nodig, individuele business units moeten dit zelf regelen. Na een aantal jaar zie je dan een veelvoud aan doublures en gaat de golfbeweging naar ‘applicatierationalisatie’ om de zoveel jaar van 1600 applicaties terug naar 800. Hier is de groei van EA nadat er een paar jaar geleden bedacht was dat dit niet meer nodig was. (bemoeials, we zoeken dit zelf wel uit)
    - Scrum teams gedragen zich dan als bataljons: ‘Gespecialiseerd in het geruisloos langs elkaar heen bewegen’
  - ‘Working systems before comprehensive documentation’
    - Oppassen dat dit niet wordt aangegerepen om maar niets aan documentatie te doen.
  - Soms zie je dat als er massaal op autonome scrum teams werd ingezet dat de samenhang der dingen verdween. Daarna is er behoefte is aan enterprise architectuur.

Architectuurcyclus

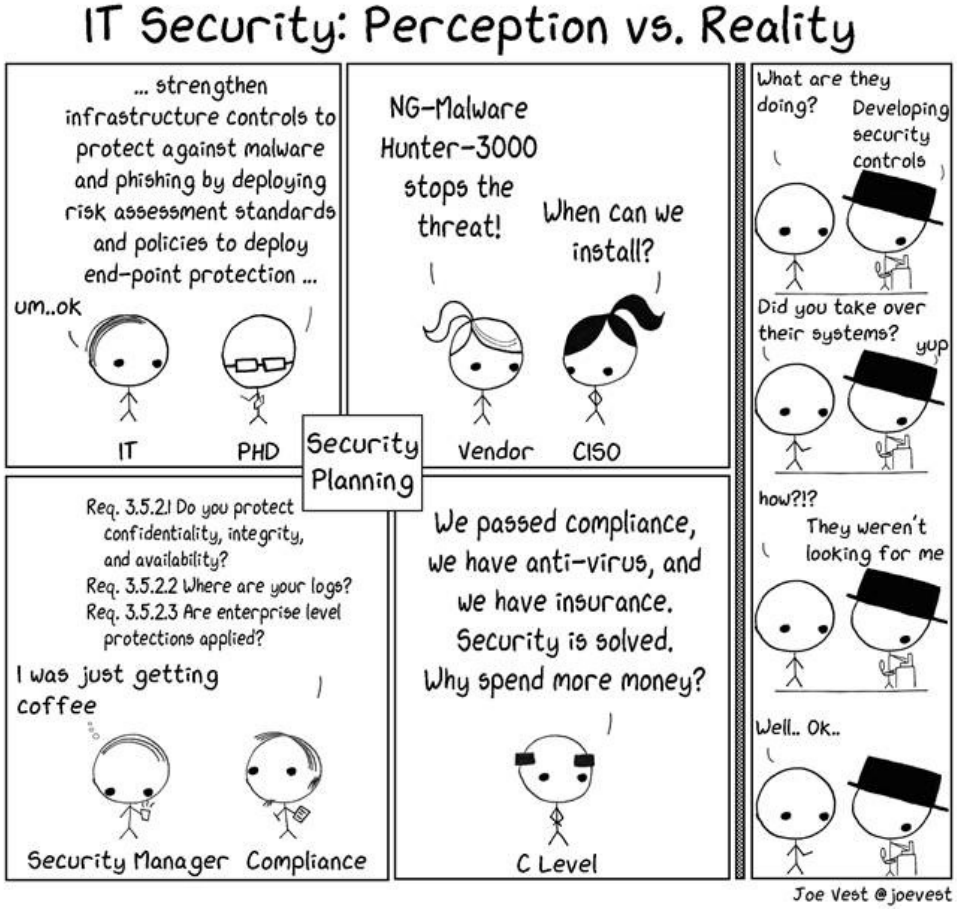
PvIB
Platform voor
InformatieBeveiliging



Disconnect

- Spanningsveld tussen Compliance en Security
  - De neiging van auditors om de wereld in een begrijpelijk (administratief) model te beschrijven zonder te verifiëren of dit model de werkelijkheid voldoende benaderd. Vergelijk compliance modellen ISO, Cobit enzv. maar eens met best practice NIST Cyber Security framework

Compliance

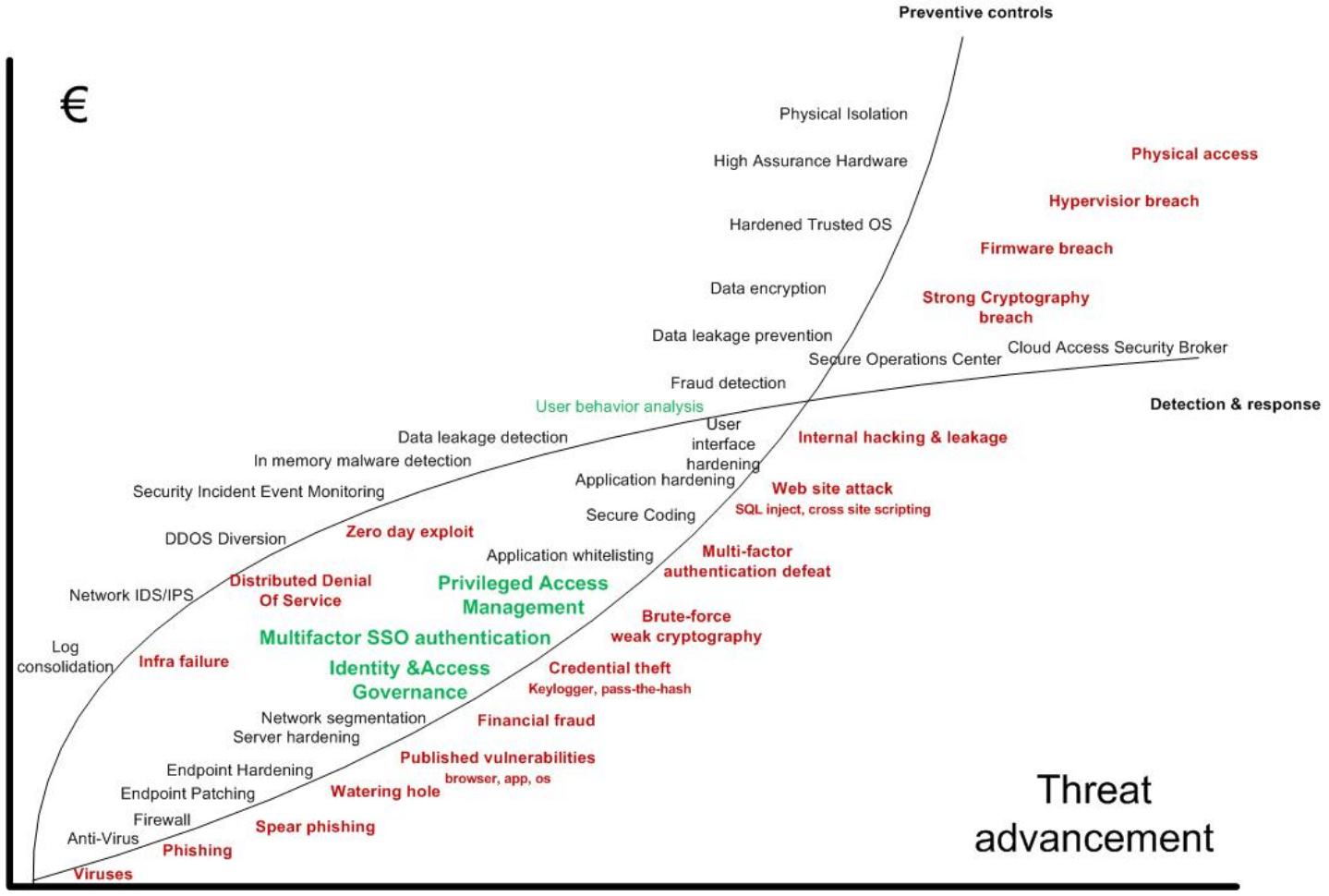


NIST CSF

Cybersecurity denkmodel

PvIB
Platform voor
InformatieBeveiliging

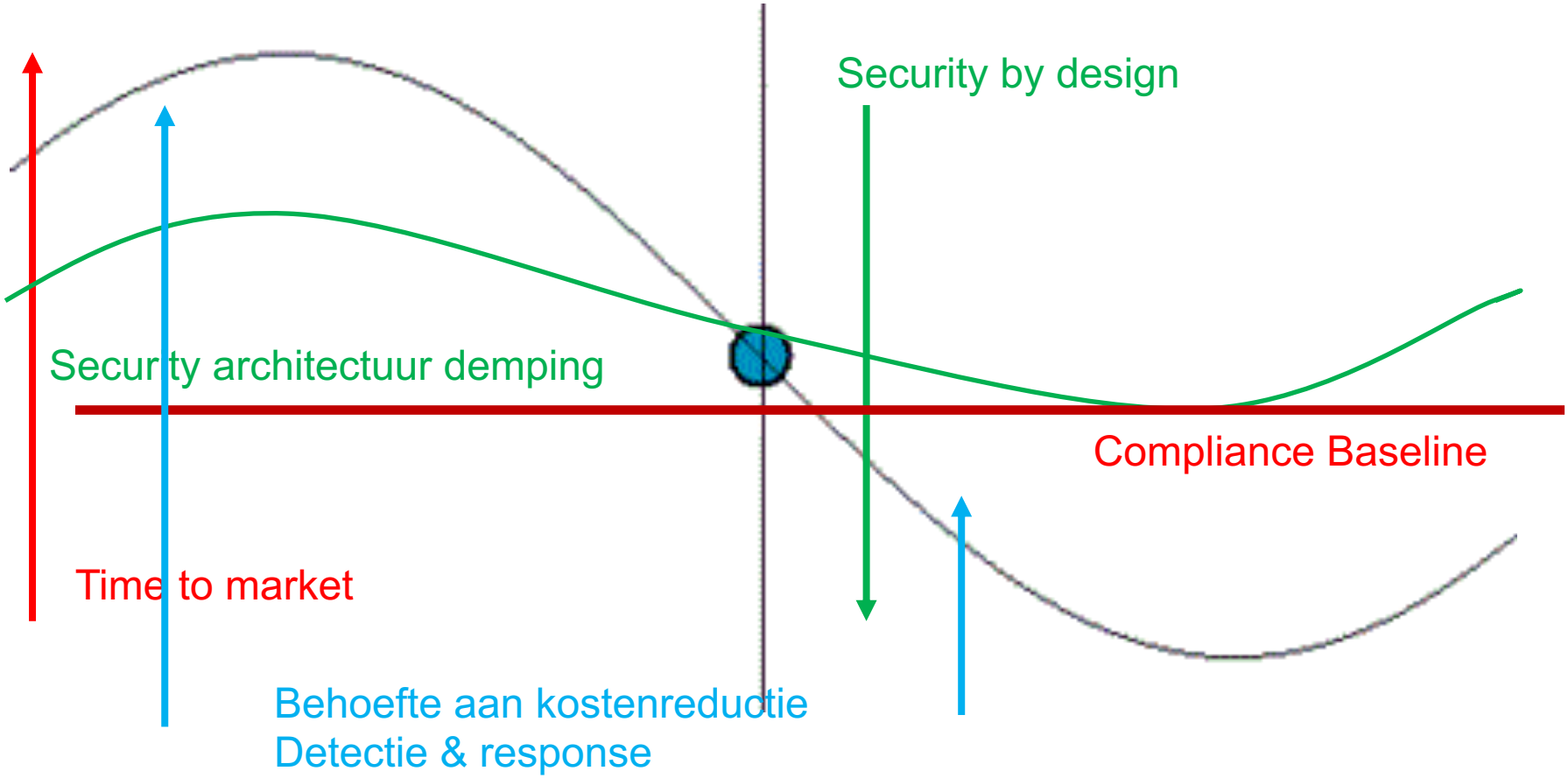
- Er is geen compliance model dat alle risico's afdekt, kortom prijsschieten voor aanvallers



Disconnect in tijd

- De golfbeweging zie ik ook in de Enterprise Security Architectuur.
- We gaan eerst voor compliance, check in the box. Of dit secure is laten we even in het midden. Omdat er steeds meer besef komt dat de aanvallen gepareerd moeten worden zie je een groei van NOC naar SOC naar CRC.
- Bij een Cyber Resilience Centre zie je dat de kosten van detectie en response oplopen en dus ontstaat er een golfbeweging naar preventie.
  Dit doe je dan toch weer door secure design te doen, maar dit keer is er een financiële business case en dan keert de golf weer.

Securitycyclus



Security toevoegen aan het model

PvIB
Platform voor
InformatieBeveiliging

- Probeer vooraf aan tafel te komen
  - Verplaats je in programmeurs die vrijheid willen en willen experimenteren
  - Ga zelf programmeren om in gesprek te blijven
  - Sterke focus op interactie, leef je in in andere belangengroepen
  - Fungeer als de wijkagent die helpt met oplossingen (design patterns) en niet als recherche
  - Word eens projectleider en voel de druk van tijd en geld
  - Werk eens in een marketing/sales setting

- Wordt traveller in Scrum teams
  - De verhaallijn gaat over persona's. introduceer een persona non grata
  - Devsecops: Opnemen van security user stories
  - De abuser story wordt dan: Ik ben hacker en ik wil …., of ik mag niet …
  - Door deze stories op te nemen in de backlog van de eerste sprint heb je gelijk je bewustwording van het scrum team en de product owner.
  - Bovendien moet de product owner ineens per sprint een afweging maken tussen functionaliteit(opportunity) en security(risk), dus gelijk belegd bij het management.
  - Introduceer de security architectuur: 'Comprehensive documentation to get working systems'

Persoonlijke Model Bloopers

- Hee riccardo: guess what, het is gelukt! De Security Architectuur Raad is akkoord!
- Omdenken: Hoe leer ik Machine learning
  - Lekker lineaire algebra met matlab e.d.
  - AI playground (Alten): maakt niet uit, het werkt. Modellen ontwikkel je niet, je gaat gewoon alle mogelijke modellen testen en kijken wat het beste werkt

•Vragen?