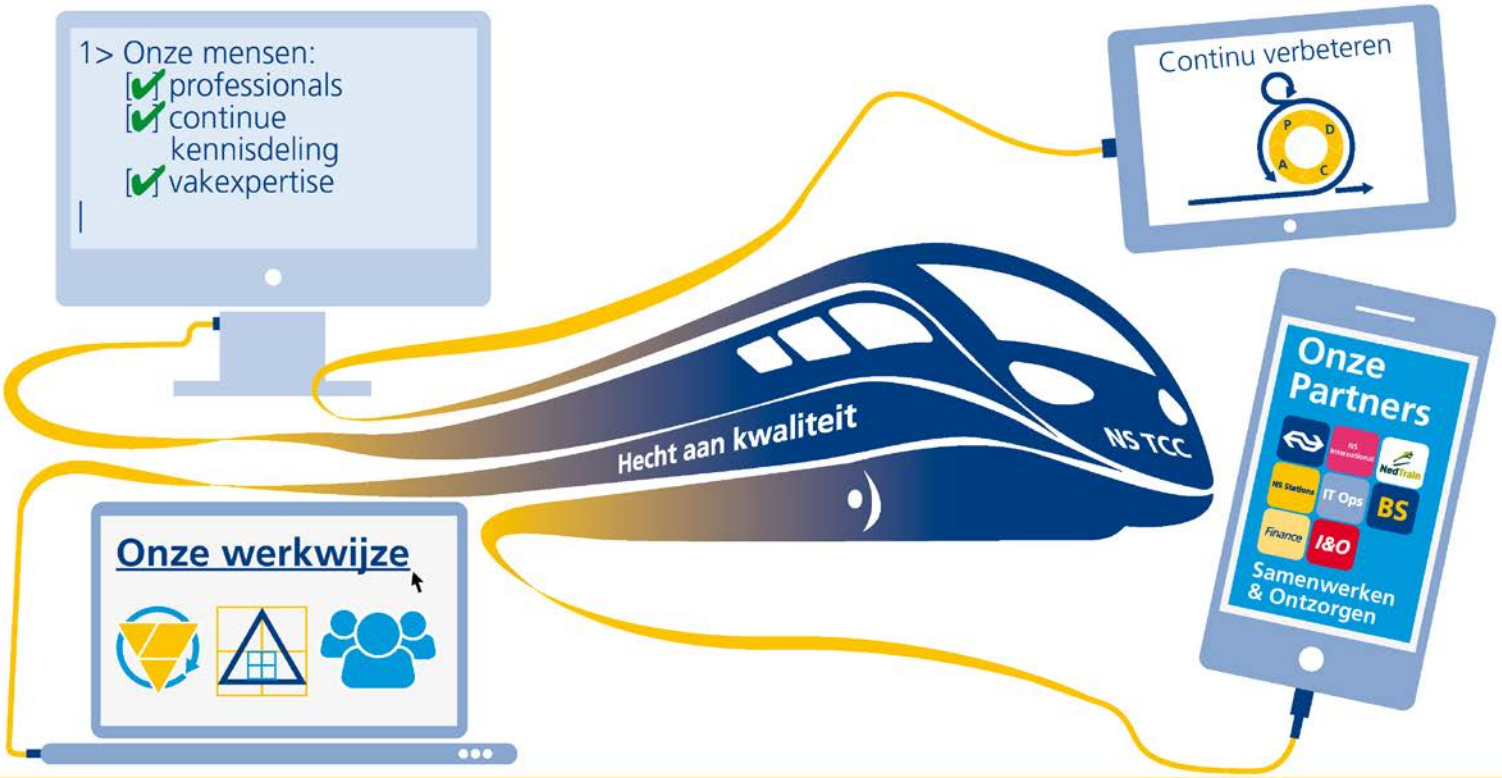
Security Testen @ NS

Onno Wierbos, Barry Schönhage, Marc Kuiper



NS Test Competence Center

Geeft helder inzicht in de risico's van software en hoogwaardig advies voor inproductiename

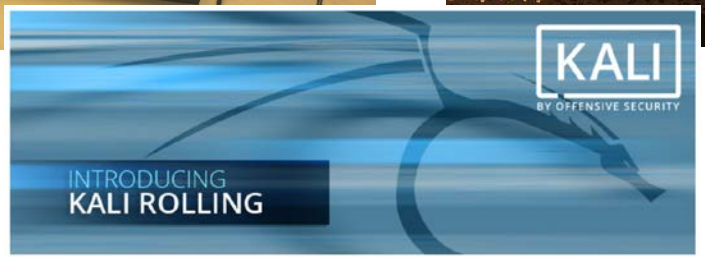
On Board Information System (OBIS)

JUST DO IT.

Security test op het nieuwe CMS

- Scope:
  - Het nieuwe CMS vanuit reizigersperspectief
  - Ik zit in de trein en maak verbinding met “Wifi in de trein”
  - Waar kan ik bij waar ik niet bij zou mogen? Voor én na het accepteren van de gebruikersvoorwaarden (captive portal)
  - OWASP (Open Web Application Security Project) TOP10
  - Blackbox approach (eigenlijk grey/white box, gezien mijn voorkennis)

Testopstelling



Kali Linux, Rolling Edition Released – 2016.1

Wat te doen met de resultaten?

Nader onderzoek:

- Tools geven hele concrete meldingen, maar ook hele vage meldingen
- Kans op False positives/negatives is behoorlijk
- Alles handmatig naspelen

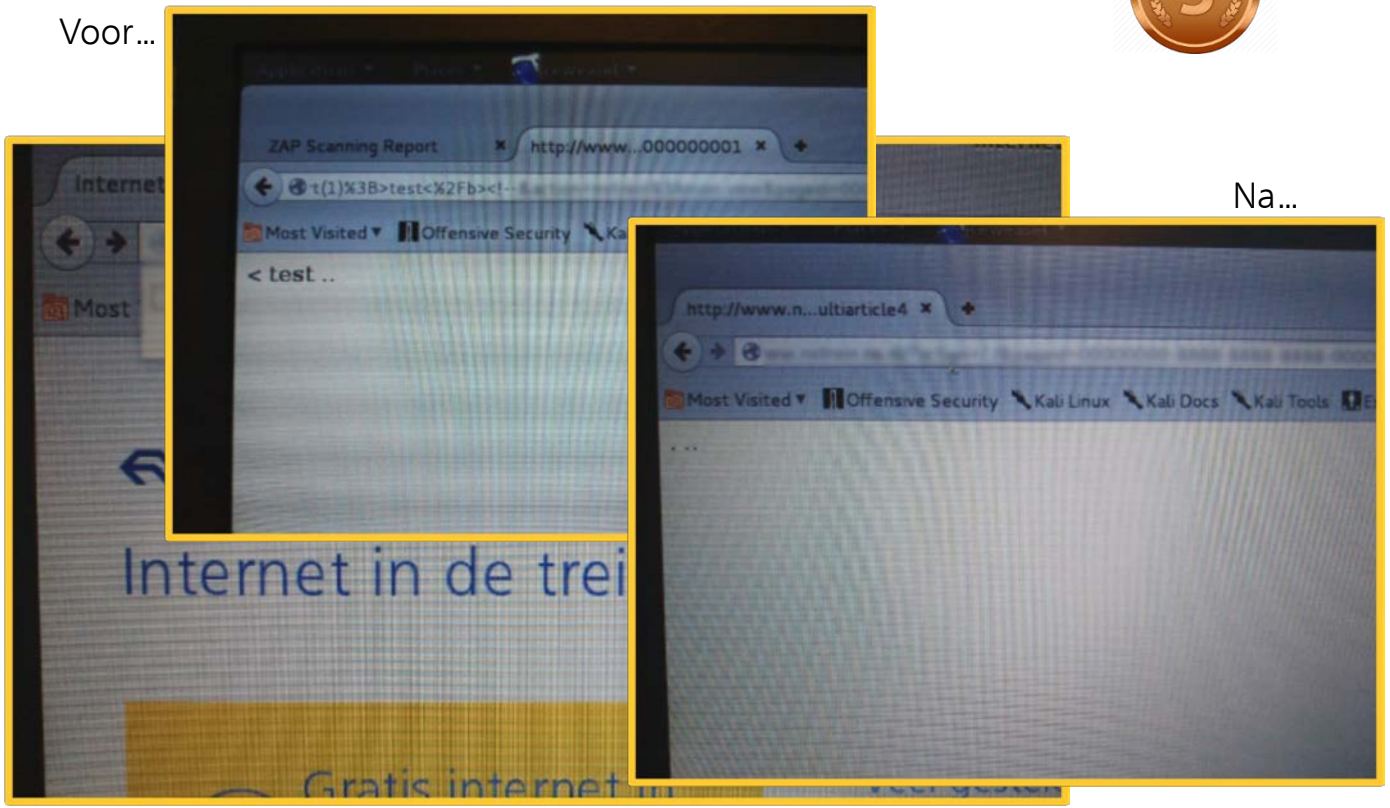
Rapporteren

- Rapportje met bevindingen
- Vastleggen in bevindingen registratie van het project, maar…
- Separate excel met details
- Versturen buiten NS? Voorzichtigheid geboden!

XSS – Cross Site Scripting “in effect”…

Voor…

Na…



Winst?

- Wat hebben we er aan?
  - We krijgen vroegtijdig al inzicht in het kwaliteitsaspect security
  - Professionalisering van het testproces
  - Beter ondersteuning van he
  - Resulterend in een hogere gen
- Maar…
  - Nog steeds onafhankelij ntest
  - Dan wel white- of zelfs
- Nog meer winst te behalen?

Interesse gewekt?

- Kali Linux tutorial op pluralsight
  https://www.pluralsight.com/courses/kali-linux-penetration-testing-ethical-hacking
- Portal met overzicht van hacktools
  https://www.concise-courses.com/hacking-tools/

Spelen?

- Bewust kwetsbare applicaties; Webgoat en Mutillidae
  https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
  https://www.owasp.org/index.php/OWASP_Mutillidae_2_Project
- Oefenenwebsite met uitdagingen van oplopend niveau
  https://www.hackthissite.org/

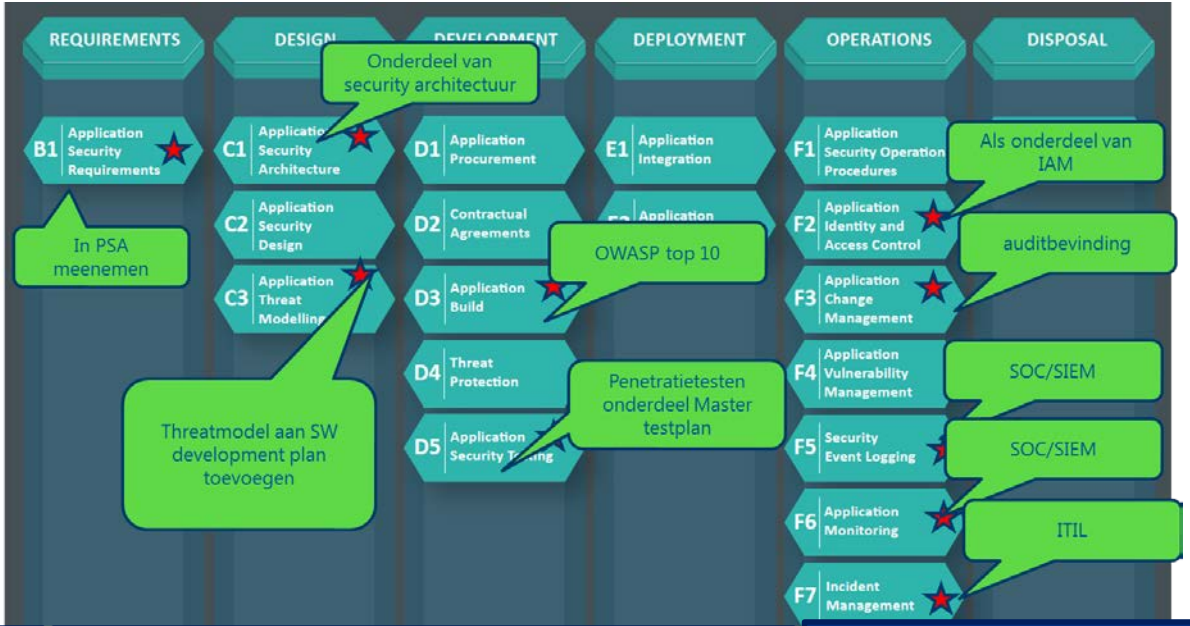

Rabobank


FREELANCER


407

Application Security Frameworks

ISF application security framework



B1 Application Security Requirements

- Business Impact Analyse (BIA)
- Privacy Impact Analyse (PIA)
- Security Beleid
- Rollen en verantwoordelijkheden

C1 Application Security Architecture

- Functioneel bijvoorbeeld > 20.000 gebruikers maak gebruik van SSO
- Moet aansluiten op de bestaande AD

C3 Threat modeling (Design)

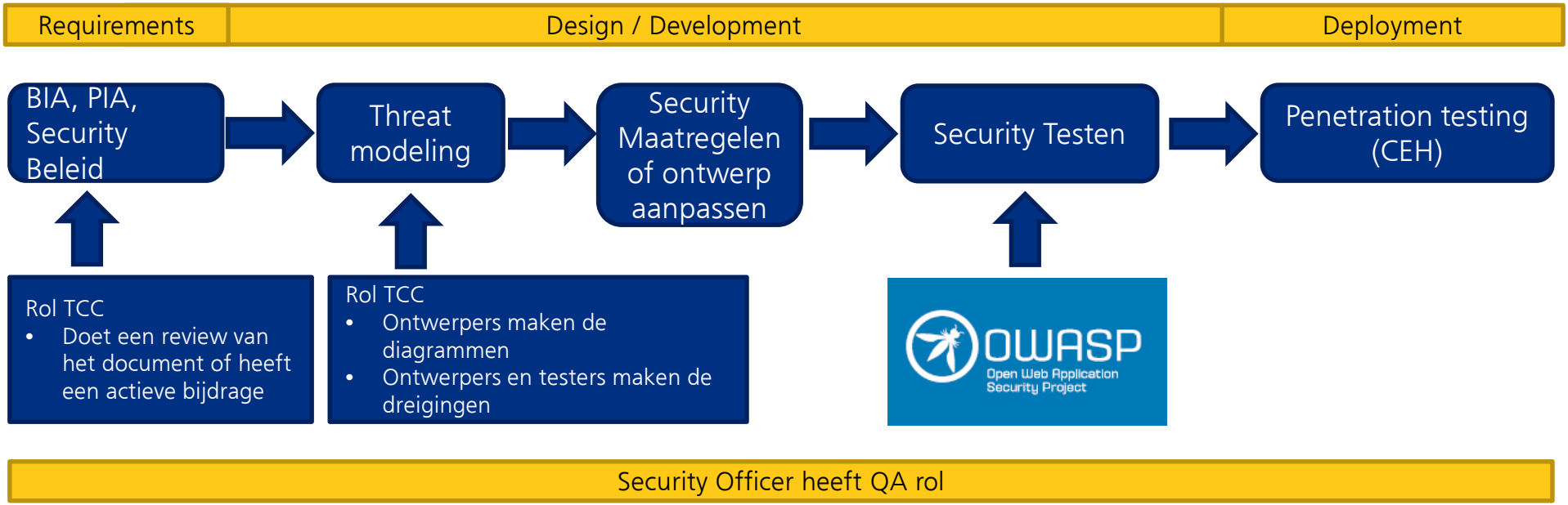
- Ontwerpers maken de diagrammen
- Ontwerpers en testers maken de dreigingen

D3 OWASP top 10 of Certified Secure checklist

D5 Application Security Testing

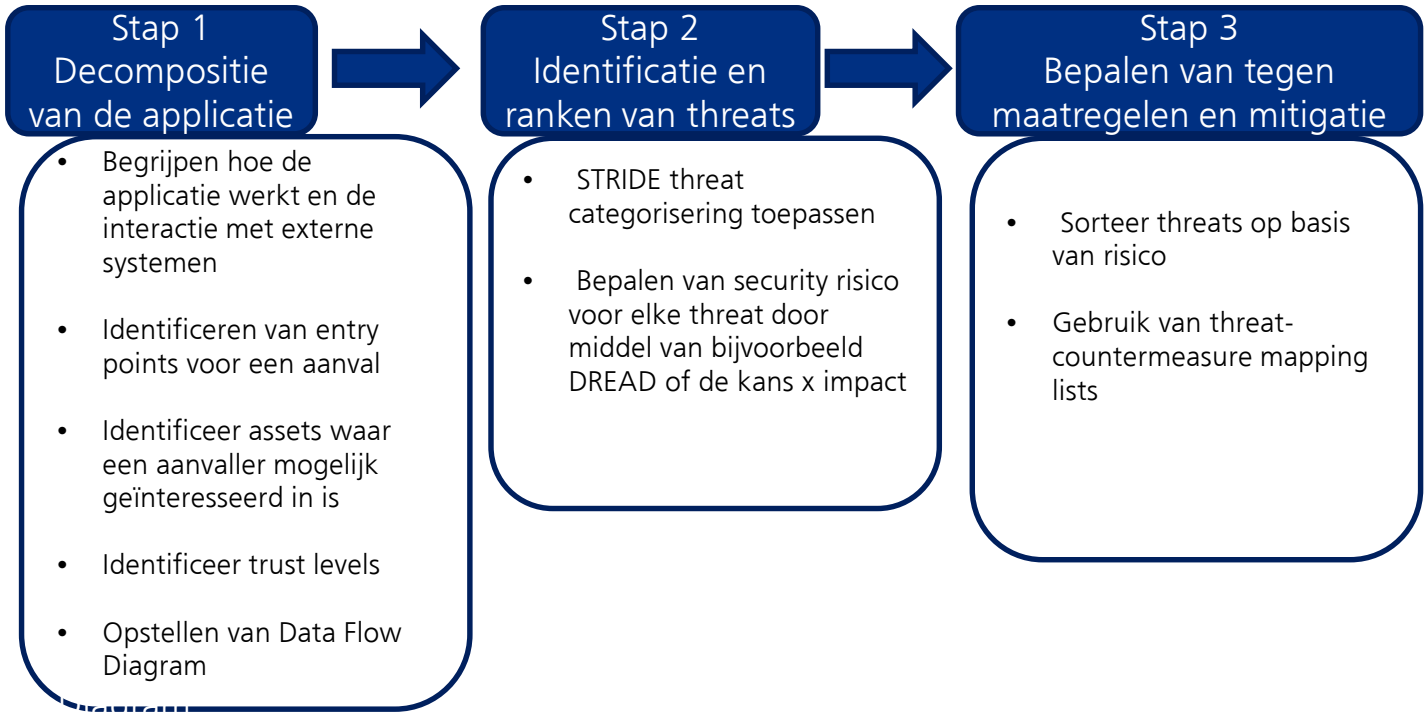
- Application Security Testing volgens OWASP Web Application Testing
- Penetratietesten intern / extern

TCC Security Test Proces

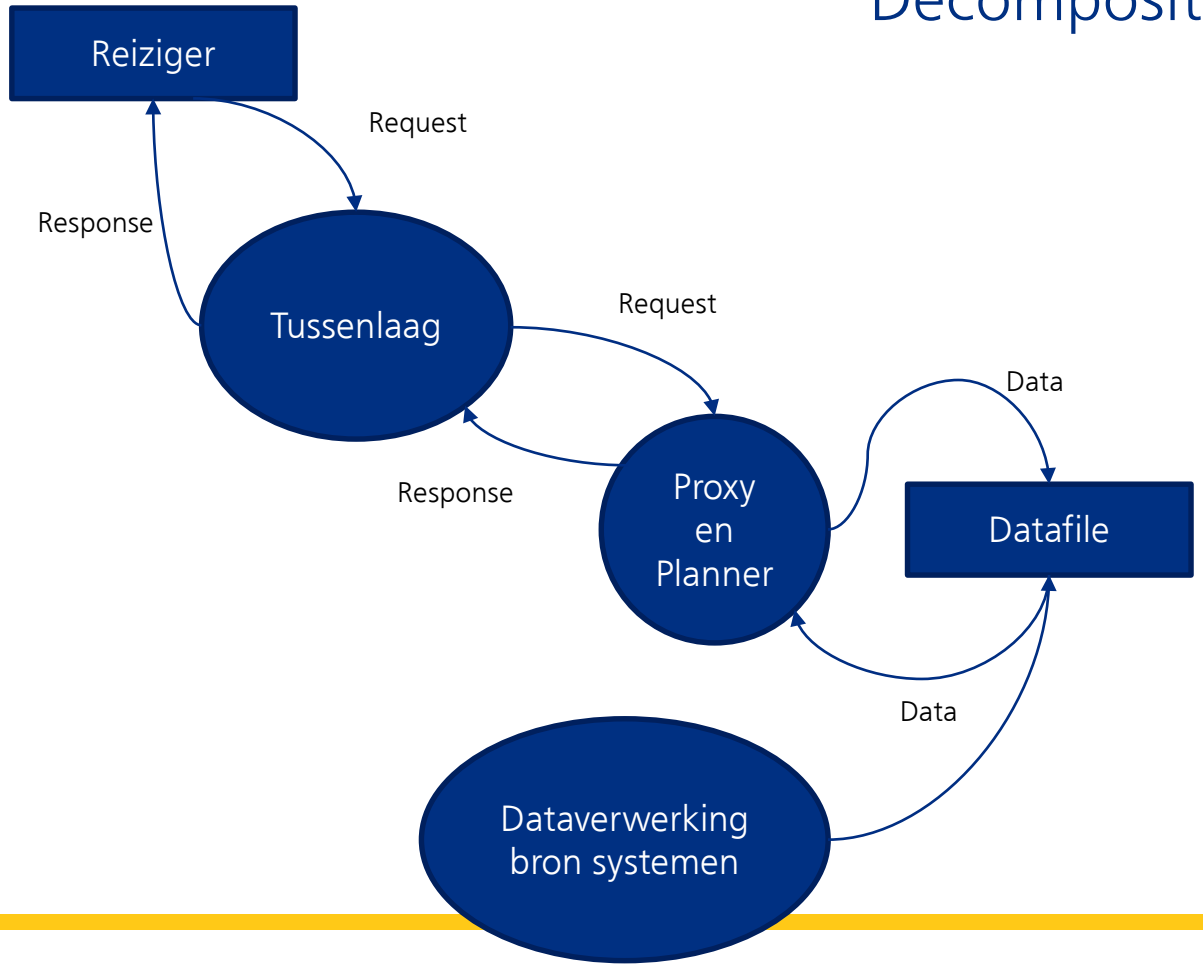


Application Threat Modeling

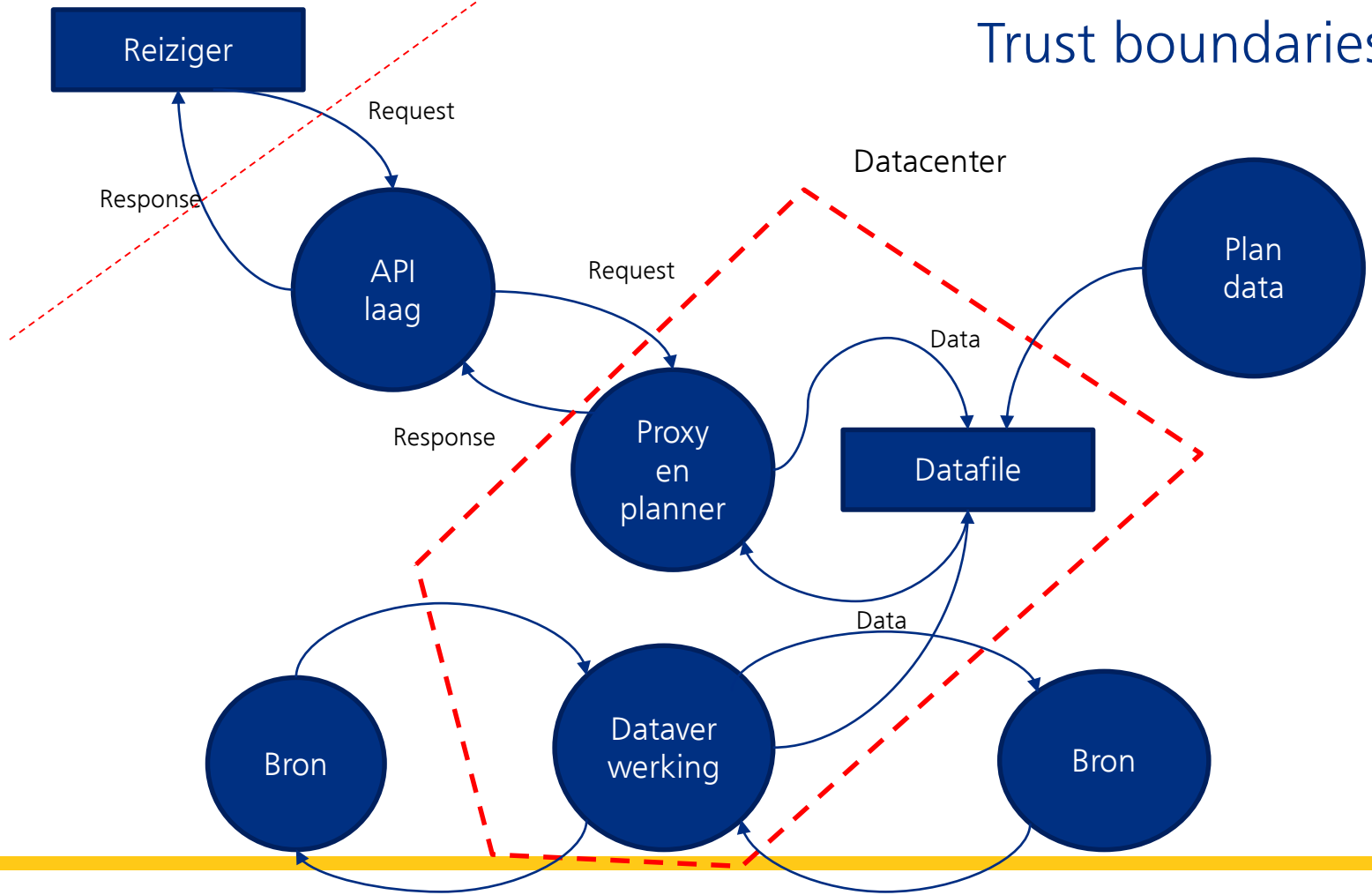
Application Threat Modeling - Stappen



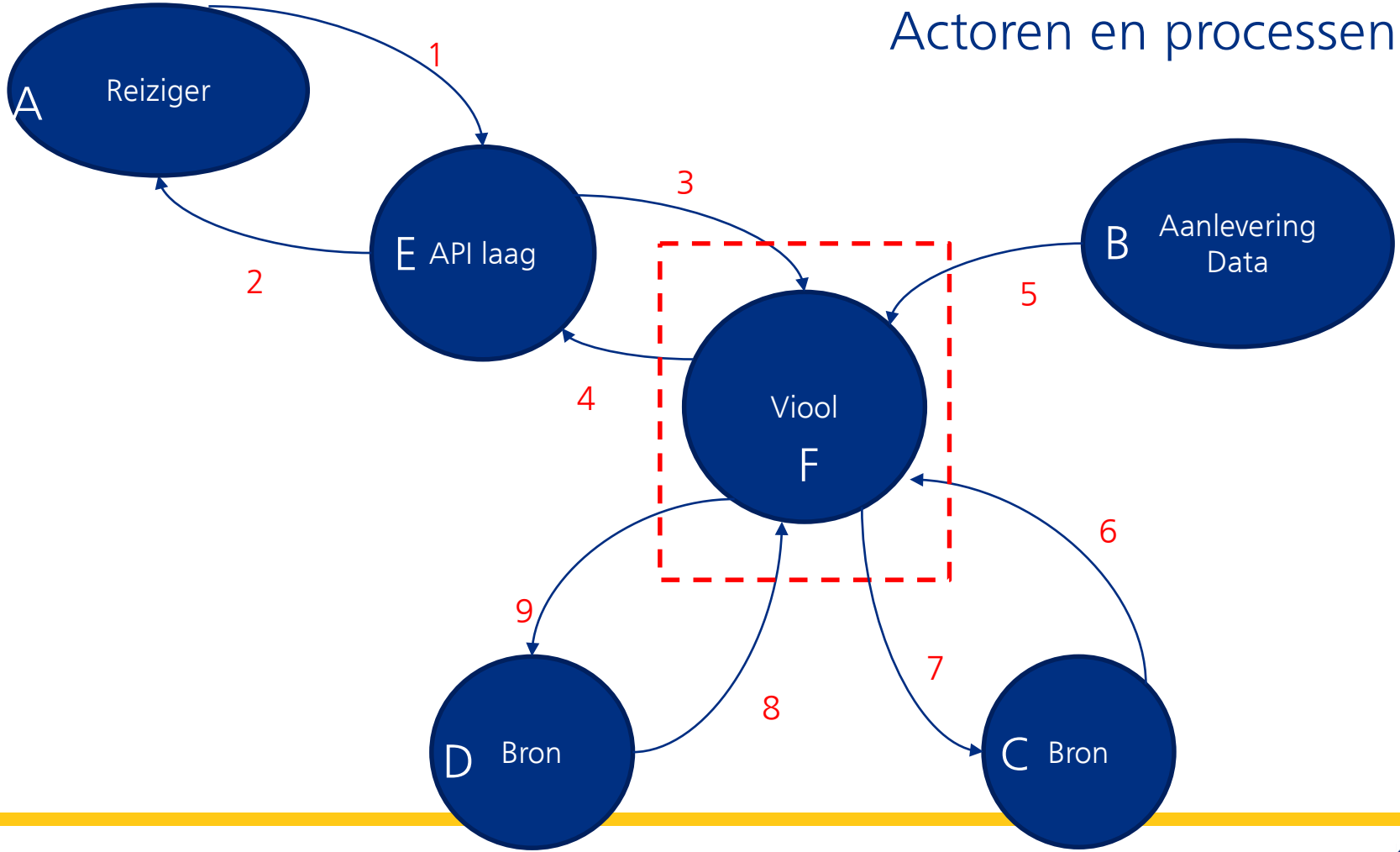
Decompositie van de applicatie



Trust boundaries



Actoren en processen



STRIDE threat list

- **S**poofing
- **T**ampering
- **R**epudiaton
- **I**nformation disclosure
- **D**enial of service
- **E**levation of priviliges

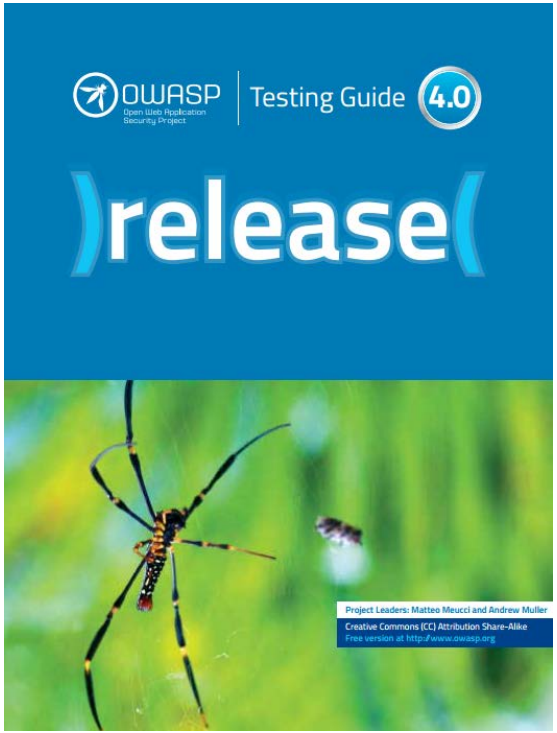
Security Control

- Authentication
- Integrity
- Non-Repudiation
- Confidentiality
- Availability
- Authorization

Bepalen van tegen maatregelen en mitigatie

- **Spoofing Identity**
  - Appropriate authentication
  - Protect secret data
  - Don't store secrets
- **Repudiation**
  - Digital signatures
  - Timestamps
  - Audit trails
- **Denial of Service**
  - Filtering
  - Throttling
  - Quality of service
- **Tampering with data**
  - Appropriate authorization
  - Hashes
  - Digital signatures
  - Tamper resistant protocols
- **Information Disclosure**
  - Authorization
  - Privacy-enhanced protocols
  - Encryption
- **Elevation of privilege**
  - Run with least privilege

Web Application Security Testing



- Configuration and Deployment
- Management Testing
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for weak Cryptography
- Business Logic Testing
- Client Side Testing

HTTPS valideren

- HTTPS protocol is gebouwd op TLS/SSL om data te encrypten
- De veiligheid hangt af van:
  - Encryptie algoritme
  - Robuustheid van de sleutels
- SSL/TLS moet goed geconfigureerd zijn

Wireshark voorbeeld / HTTPS test voorbeeld

TCC Security Test Proces