SQUALIO

SOFTWARE QUALITY ASSURANCE

Programmatūras kvalitātes nodrošināšana un testēšana informācijas sistēmu drošībai

Nikolajs Petrovs

SQUALIO
SOFTWARE QUALITY ASSURANCE

AKTĪVA PIEEJA INFORMĀCIJAS SISTĒMU DROŠĪBAI

- Potenciālos drošības draudus jāsāk risināt jau programmatūras izstrādes fāzē
- Jāskatās SDLC virzienā (drošas izstrādes programmatūras dzīves cikls)
  - Kvalitātes nodrošināšana
  - Drošība

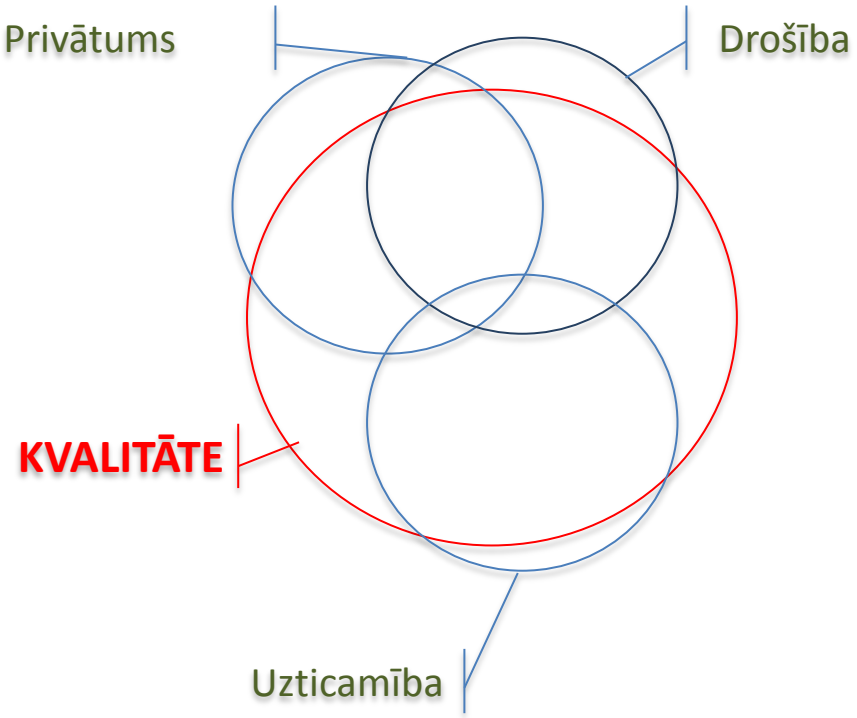
SQUALIO
SOFTWARE QUALITY ASSURANCE

PROGRAMMATŪRAS IZSTRĀDES PAŅĒMIENI

- Atvērtā koda (open-source) tipa projekts
- Formālākas metodes
  - Ūdenskrituma modelis
  - Spirāles modelis
  - CMMI (Capability Maturity Model Integration)
  - TSP – Team Software Process
  - PSP – Personal Software Process
- Agile
- Common Criteria (zināmi arī kā ISO/IEC 15408)
  - Novērtējuma līmeņi - Evaluation Assurance Levels (EAL)

SQUALIO
SOFTWARE QUALITY ASSURANCE

KVALITĀTES ASPEKTI



- Kvalitātes problēmas ir kopīgas
  - Privātums
  - Drošība
  - Uzticamība
- Drošības ieroči
  - Tīrs kods
  - Atbilstoša konfigurācija
  - Drošības produkti
- Labāk ātrāk
  - Ir par vēlu, ja vājās puses tiek iekļautas Beta versijā
  - Ir par vēlu, ja problēmas tiek atklātas tikai testēšanas laikā

SQUALIO
SOFTWARE QUALITY ASSURANCE

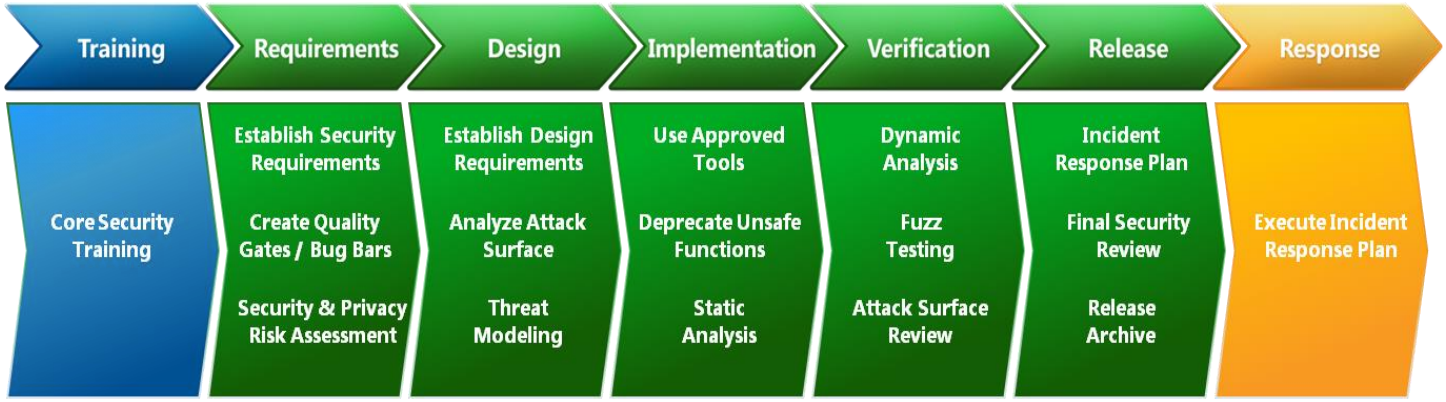
DROŠĪBAS ASPEKTI

- DROŠAS PROGRAMMATŪRAS KONCEPCIJAS
  - Konfidencialitāte, integritāte, pieejamība, autentifikācija, autorizācija un auditācija
  - Drošas izstrādes principi
  - Risku pārvaldība (piem. ievainojamības, ielaušanās)
  - Regulas, privātums un atbilstības
  - Programmatūras arhitektūra
  - Juridiskie aspekti (piem. autortiesības, preču zīmes)
  - Standarti (piemēram, ISO 2700x, OWASP)
  - Drošības modeļi (piem. Bell-LaPadula, Clark-Wilson & Brewer-Nash)
  - Droša darbināšana (piem. TPM, TCB)

SQUALIO
SOFTWARE QUALITY ASSURANCE

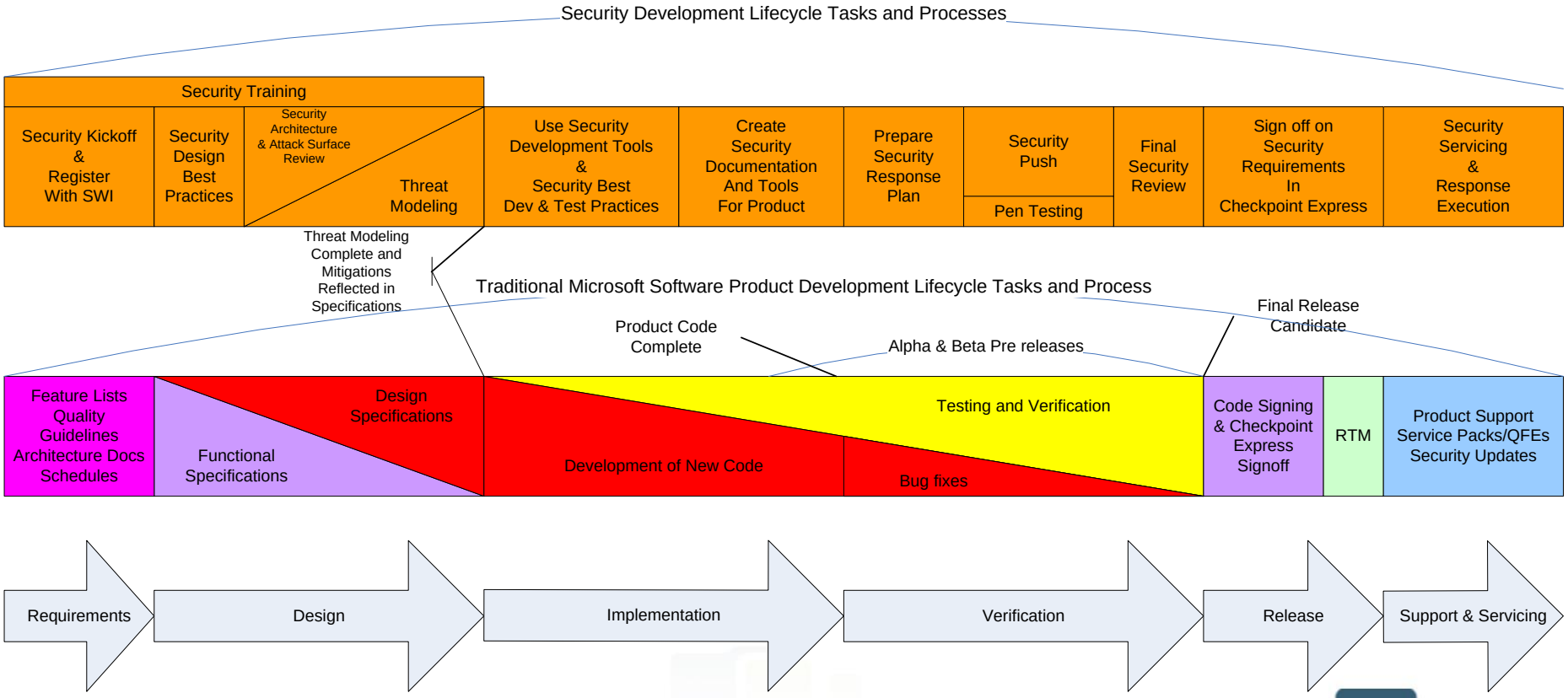
MICROSOFT DROŠĪBAS IZSTRĀDES DZĪVES CIKLS (SDL – Secure Development Lifecycle)

- Mērķi
  - Samazināt drošības trūkumu un privātuma problēmu skaitu
  - Samazināt atlikušo trūkumu ietekmi
- SDL aspekti
  - Izglītība
  - Procesi
  - Atbildības



SQUALIO
SOFTWARE QUALITY ASSURANCE

SDL PROCESS



SQUALIO
SOFTWARE QUALITY ASSURANCE

DROŠA PROGRAMMATŪRAS TESTĒŠANA

- Testēšana kā kvalitātes nodrošināšana
  - Funkcionālā un Nefunkcionālā testēšana (piem. loģika, uzticamība, veiktspēja un mērogojamība)
  - Drošības testēšana (piem. baltās kastes un melnās kastes tehnikas)
  - Kļūdu uzskaite (piem. nepilnības, kļūdas un ievainojamības)
  - Uzbrukuma virsmas validēšana (Attack surface validation)
- Testēšanas veidi
  - Ielaušanās testēšana
  - «Fuzzing», «Scanning», simulētā testēšana (piem. videi un datiem)
  - Šifrēšanas validēšana (piem. videi un datiem)
- Regresijas testēšana

SQUALIO
SOFTWARE QUALITY ASSURANCE

KĀ IEVIEST SDL

- Pieejamie bezmaksas rīki
  - SDL izstrādes pārvaldības vadlīniju apraksts (SDL Development Guidance)
  - SDL rīki (Attack Surface Analyzer, Threat Modelling Tool, Fuzzing Tool)
  - SDL veidnes Visual Studio Team sistēmāi (iesk. Agile)
- Microsoft pakalpojumi: Drošu produktu izstrādes pakalpojumi
  - Drošu aplikāciju izstrādes apmācības
  - Aplikāciju drošības koda pārskats
  - Aplikāciju drošības novērtējums
  - Aplikāciju draudu modelēšana
- Partneri - SQUALIO: QA&SDL konsultācijas, apmācības, testēšana
  - QA procesu novērtējums un uzlabošana
  - Koda izskatīšana
  - Testēšana

SQUALIO
SOFTWARE QUALITY ASSURANCE

Certified Secure Software Lifecycle Professional (CSSLP^{CM})

- Sertifikācija no ISC®
- Industrijas atbalsts
  - Microsoft, Cisco, Xerox, SAFECode
  - Symantec, BASDA, SANS, DSCI (NASSCOM)
  - SRA International, ISSA
- CSSLP CBK darbības sfēras
  - Drošas programmatūras koncepcijas
  - Drošas programmatūras prasības
  - Drošas programmatūras projektējums
  - Drošas programmatūras izstrāde/ieviešana
  - Drošas programmatūras testēšana
  - Programmatūras akceptēšana
  - Programmatūras uzstādīšana, uzturēšana un likvidēšana

CSSLP
Certified Secure Software Lifecycle Professional

SQUALIO
SOFTWARE QUALITY ASSURANCE

RESURSI

- Grāmatas
  - Michael Howard, Steve Lipner, The Security Development Lifecycle, 2006
  - Michael Howard, Steve Lipner, Writing Secure Code, Second Edition, 2003
  - Software Assurance Maturity Model (SAMM) , By OpenSAMM Project (OWASP)
- Interneta resursi
  - ISC2 CSSLP certification www.isc2.org/csslp
  - Microsoft SDL http://www.microsoft.com/security/sdl/default.aspx
  - The Open Web Application Security Project (OWASP) https://www.owasp.org/

SQUALIO
SOFTWARE QUALITY ASSURANCE

PALDIES PAR UZMANĪBU!

Nikolajs Petrovs
Pakalpojumu attīstības vadītājs
GSM: +371 2 912 4882
E-pasts: Nikolajs.Petrovs@squal.io
Skype: nikolay.ptrv
www.squal.io