



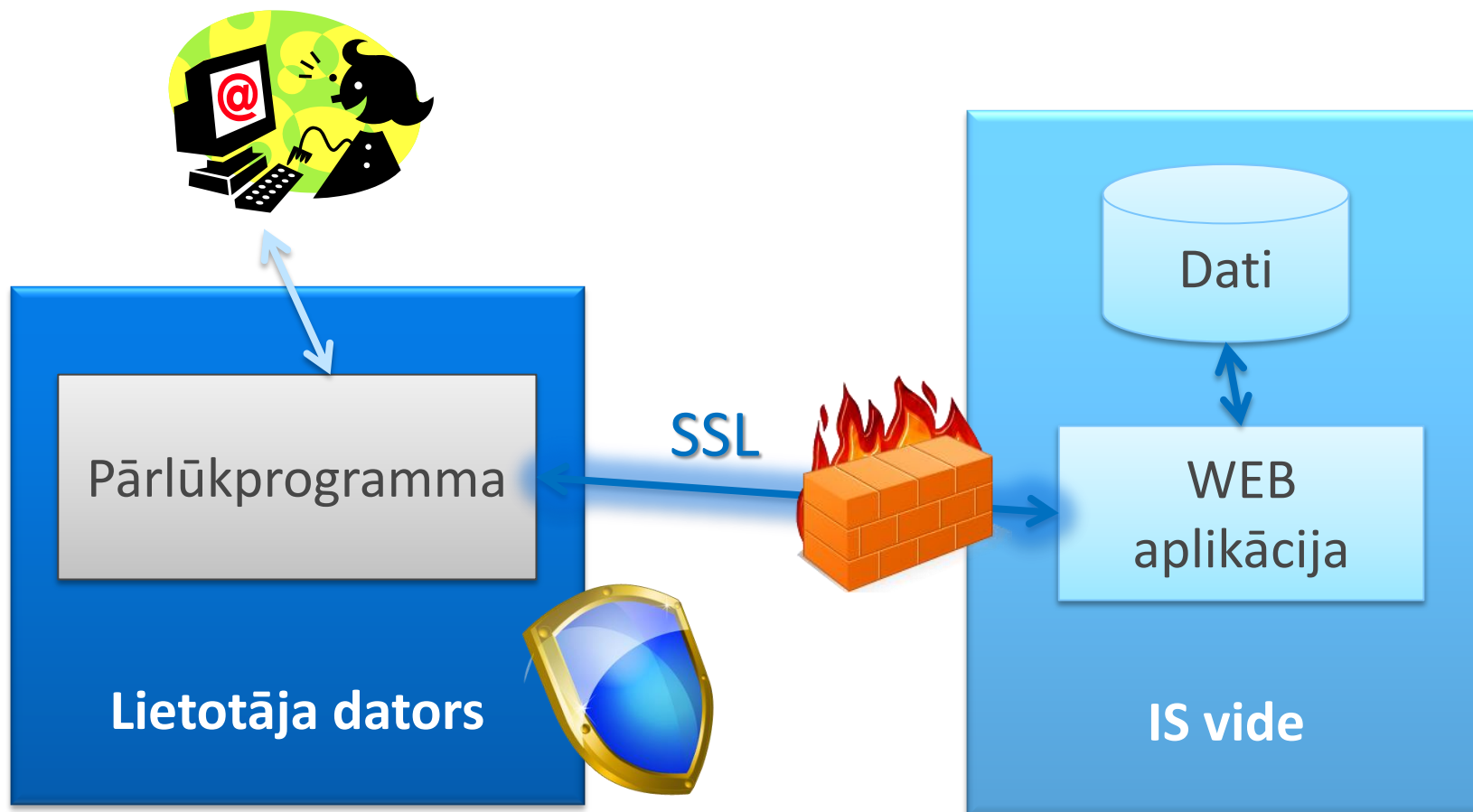
Preventīvās metodes WEB Aplikāciju drošības uzlabošanai

Ainārs Galvāns

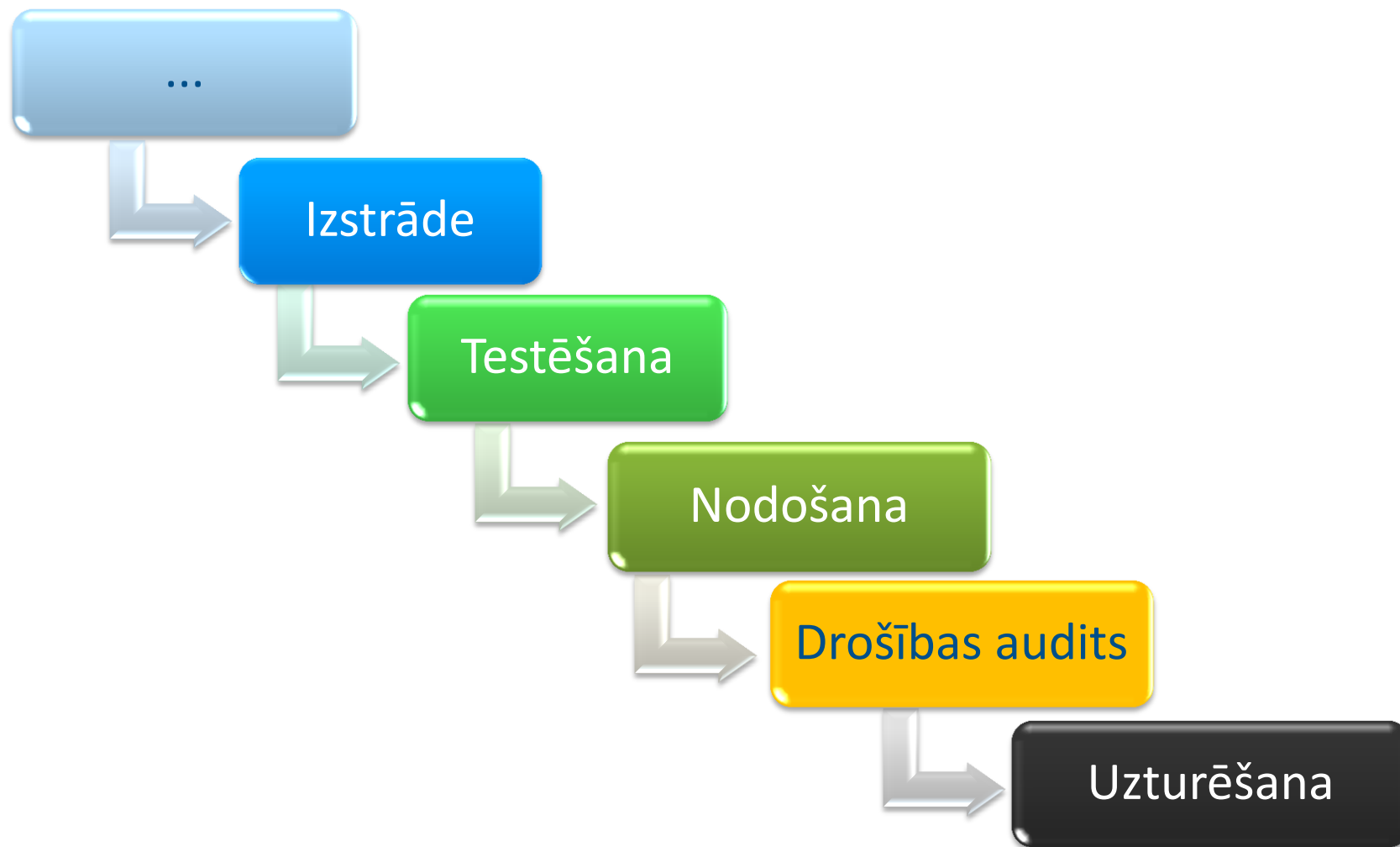
Risinājumu drošības speciālists

Exigen Services Latvia

IS drošība



IS drošības audits

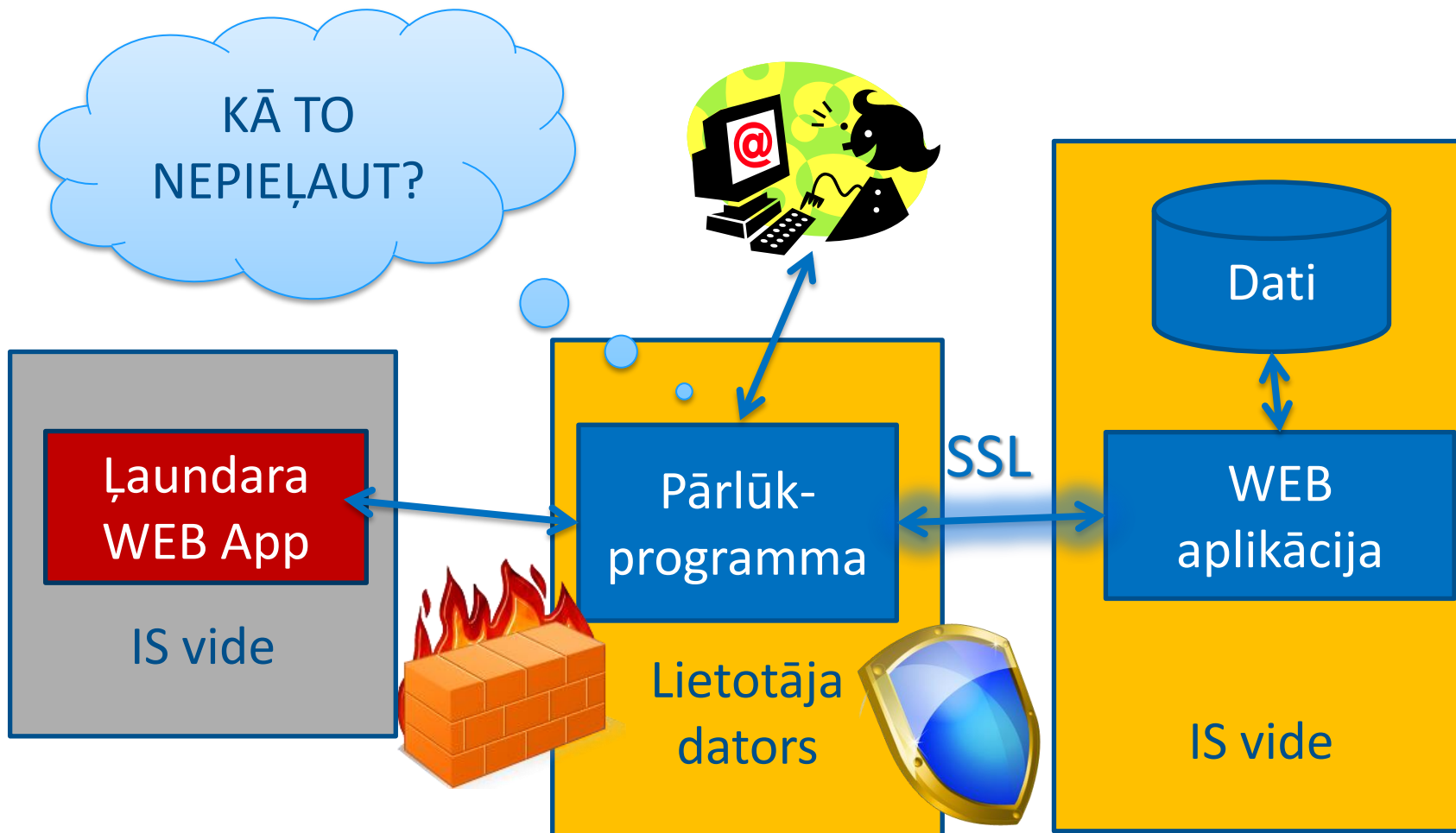


OWASP top 10 ievainojamības risku konteksts

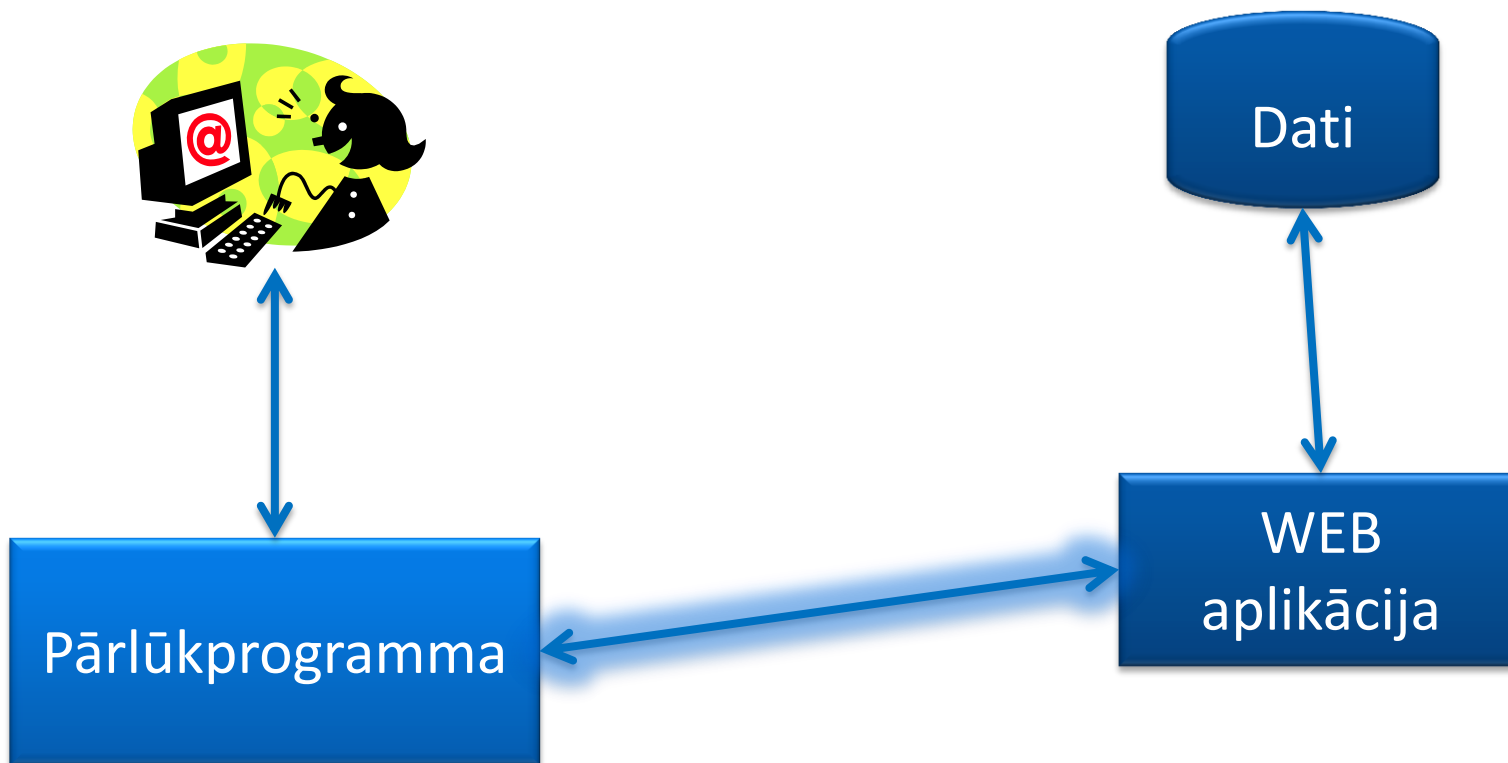
Ievainojamības Risks	WEB Aplikācija	IS konteksts
1. Injections	✓	
2. Broken authentication and session management	✓ Daļēji	✓ Daļēji
3. Cross Site scripting	✓	
4. Insecure direct access	✓	
5. Security Misconfiguration		✓
6. Sensitive data exposure		✓
7. Missing access control	✓	
8. Cross Site Request Forgery	✓	
9. Known vulnerabilities	✓	
10. Unvalidated redirects	✓	

Intranet IS – vai esam drošībā aiz ugunssmūra?

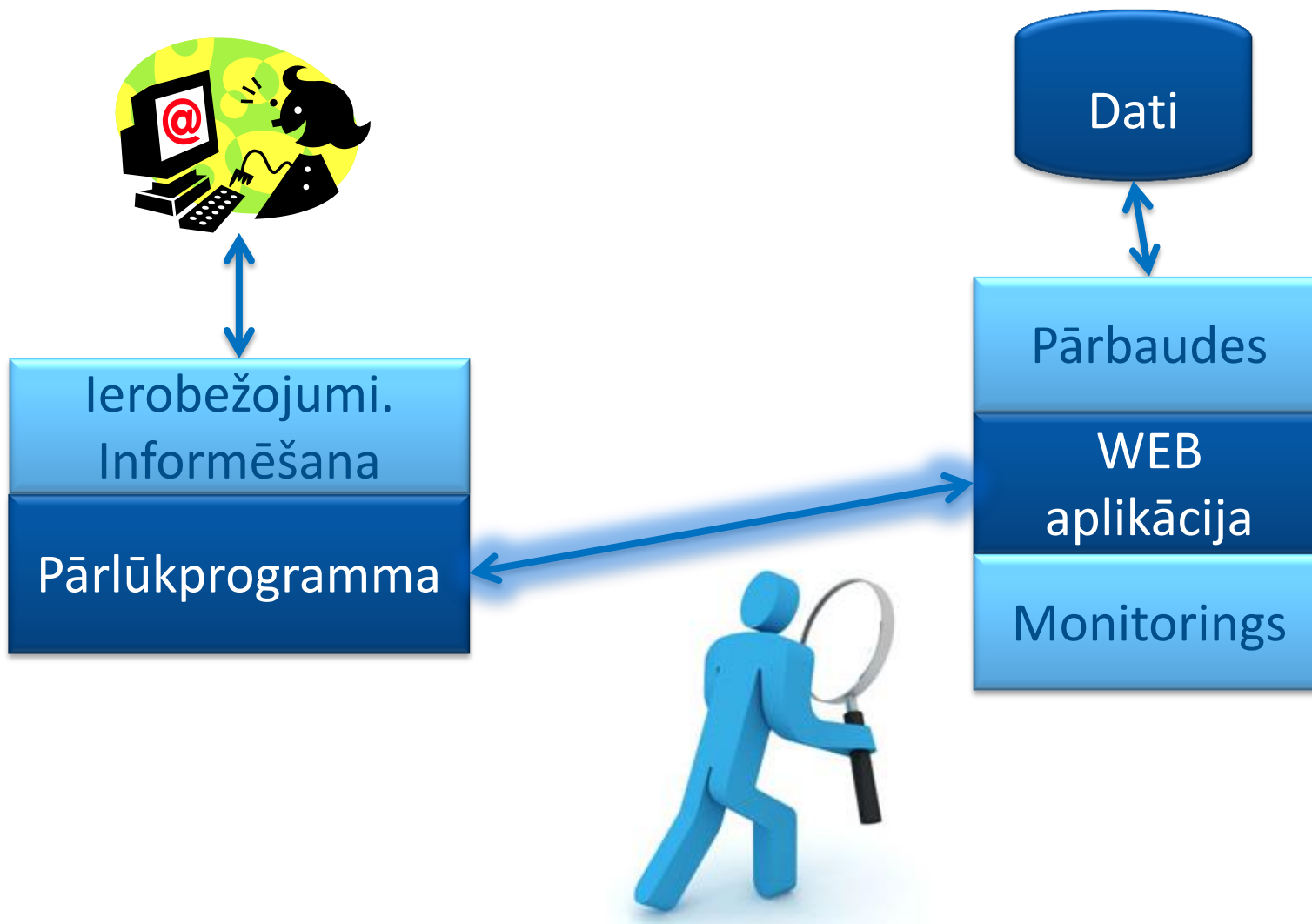
KĀ TO
NEPIEĻAUT?



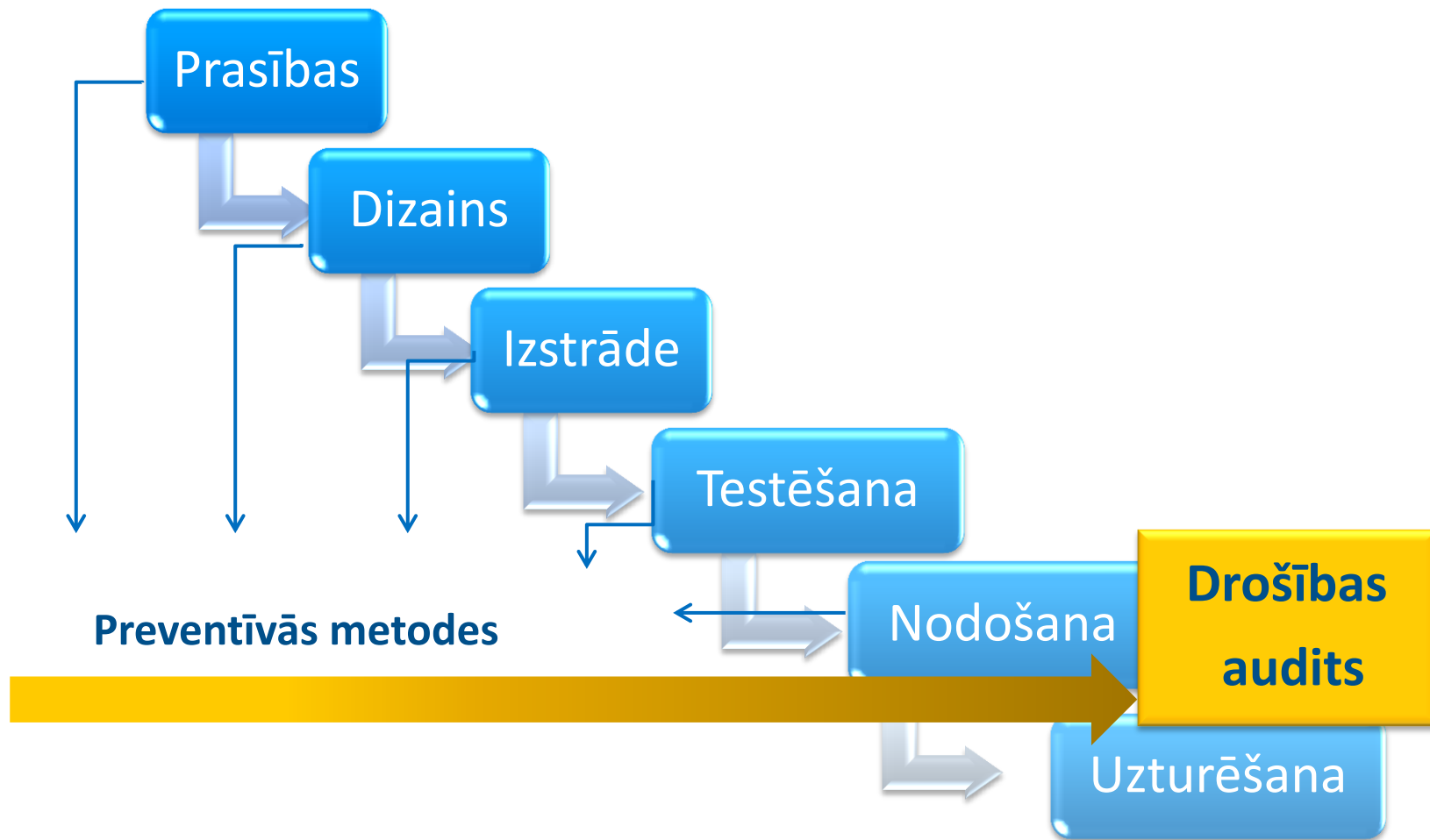
Drošas WEB aplikācijas izstrāde



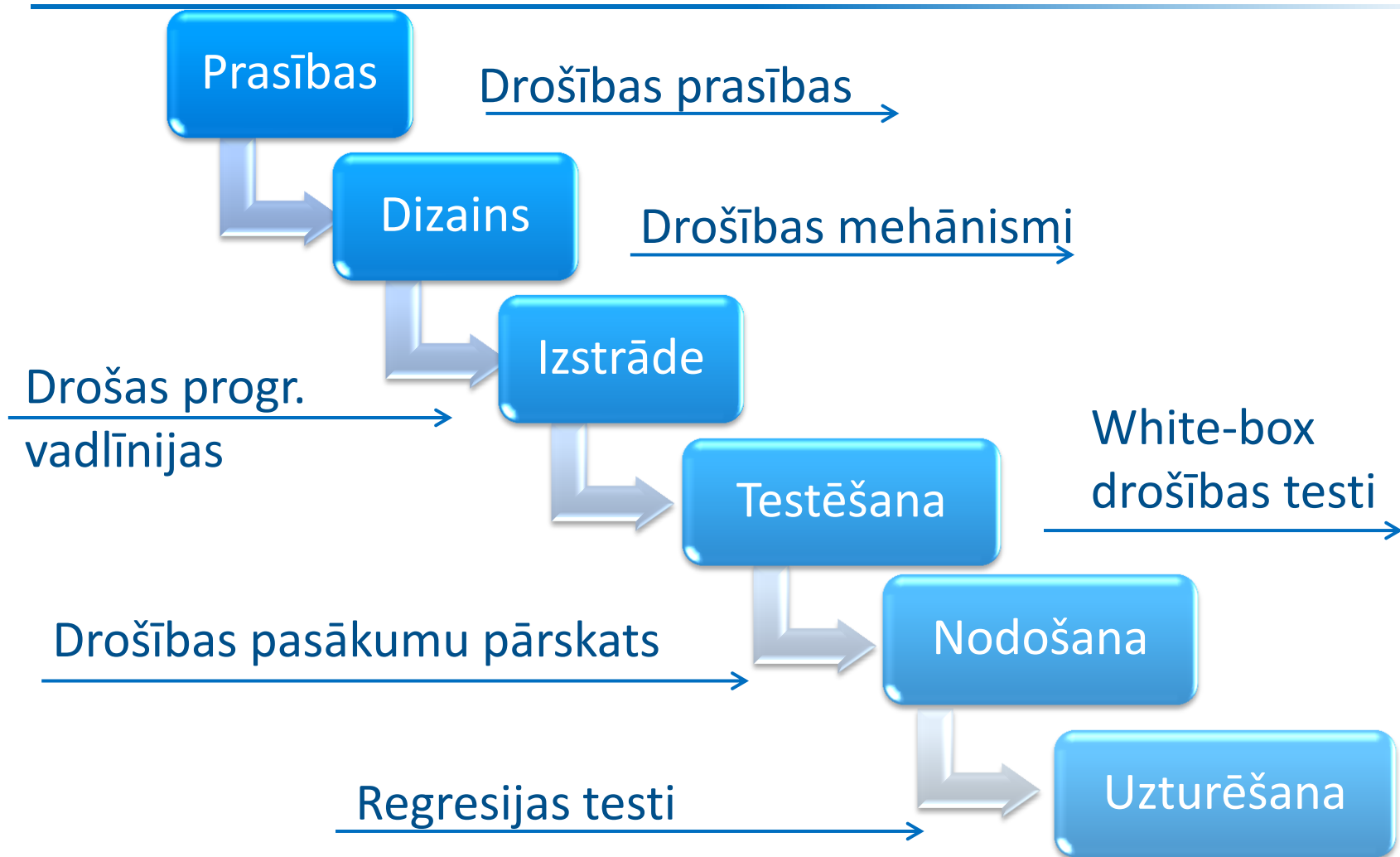
Drošas WEB aplikācijas izstrāde



WEB aplikāciju drošība



Preventīvo metožu klāsts



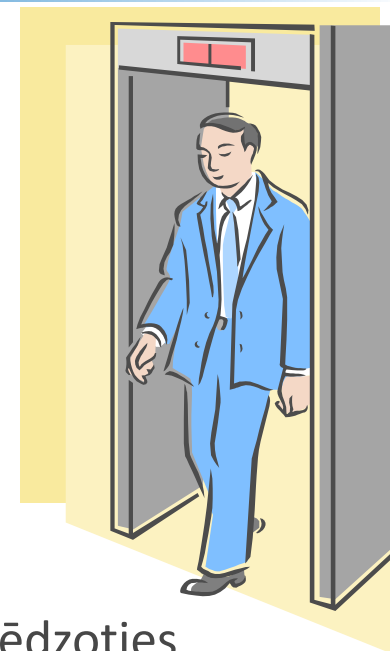
Drošības prasības

- Likumdošanas izpēte attiecībā uz drošības prasībām
 - Personas datu aizsardzības likums
 - MK noteikumi
 - Eiropas direktīvas
- Glabājamo datu un piedāvāto servisu drošības kategorija
 - Vai var veikt naudas transakcijas?
 - Vai veiktās transakcijas var ietekmēt cilvēku dzīvību, veselību?
 - Kādas var būt sekas (nelegāli) veiktām transakcijām?
 - Vai IS satur konfidenciālus datus? Kādas var būt noplūdes sekas?
 - Vai IS satur informāciju, kuras zudums, izmaiņas var nest finansiālus labumus uzbrucējam?



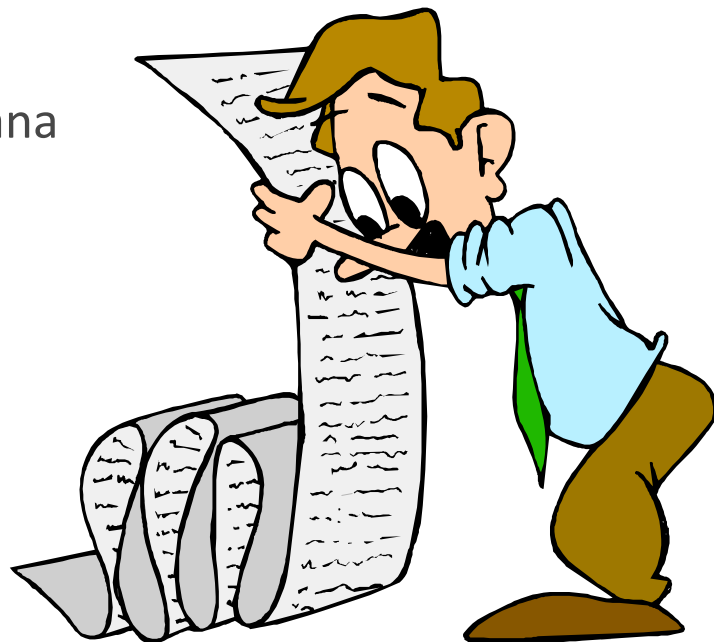
Drošības mehānismi

- Labi zināmie mehānismi:
 - Paroles sarežģīta, piespiedu nomaiņa, u.c.
 - Pagaidu bloķēšana pēc X nepareizu parolu ievades
 - Nelietotas sesijas pārtraukšana
 - CAPTCHA
 - Detalizēts notikumu audits
- Retāk lietoti mehānismi
 - Pēdēja logina informācijas attēlošana lietotājam pieslēdzoties
 - Aizdomīgu lietotāja darbību monitorēšana
 - Alternatīvs lietotāja notificēšanas kanāls, kas lietots, lai informētu par šī lietotāja veiktajām darbībām



Drošas programmēšanas vadlīnijas

- Programmētāju izglītošana
- Pārdomāta aizsardzība pret tipiskajiem uzbrukumumu veidiem
 - Ievaddatu validācija
 - Atspējot datu iegaumēšanu pārlūkā, kur tas nav nepieciešams
 - Izvaddatu enkodēšana (lai nepieļautu neparedzētu skriptu izpildi)
 - Droša sesiju pārvaldība
 - Spēcīgu kriptogrāfisko funkciju pielietošana
 - u.c.



Drošības testu iedalījums

	Black Box	Grey Box	White Box
Primāri analizē	Strādājošo aplikāciju	Biznesa loģiku, nefunkcionālās prasības	Arhitektūru un drošības mehānismus
Mērķis – pārbaudīt	Zināmos drošības «caurumus»	Biznesa riskus/draudus	Implementācijas nepilnības
Priekšnosacījumi	Rīki un to lietošanas prasmes	Biznesa izpratne (no drošības aspekta)	leviešanas pārzināšana

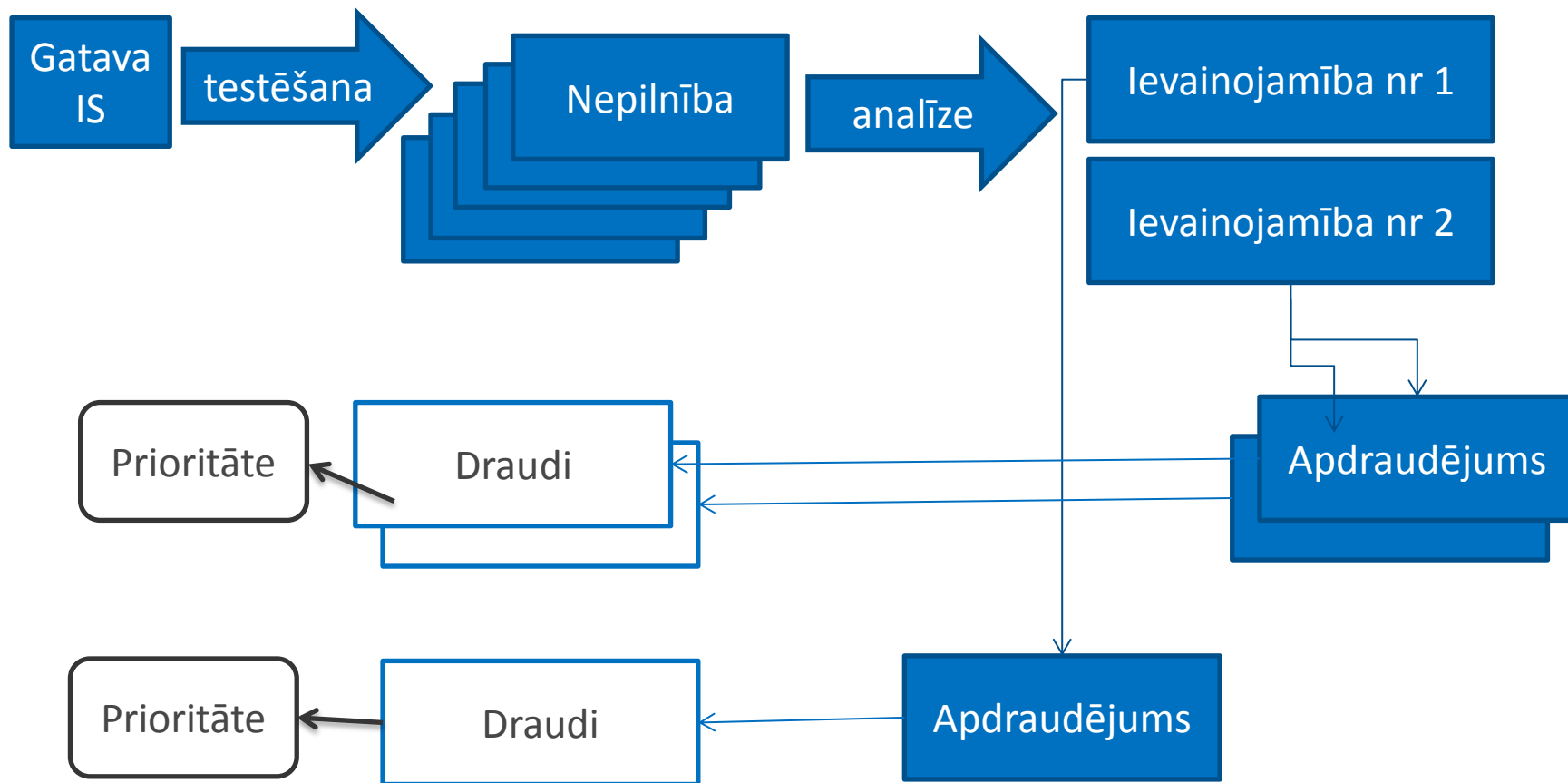
Iekšējā testēšana

Neatkarīgais audits

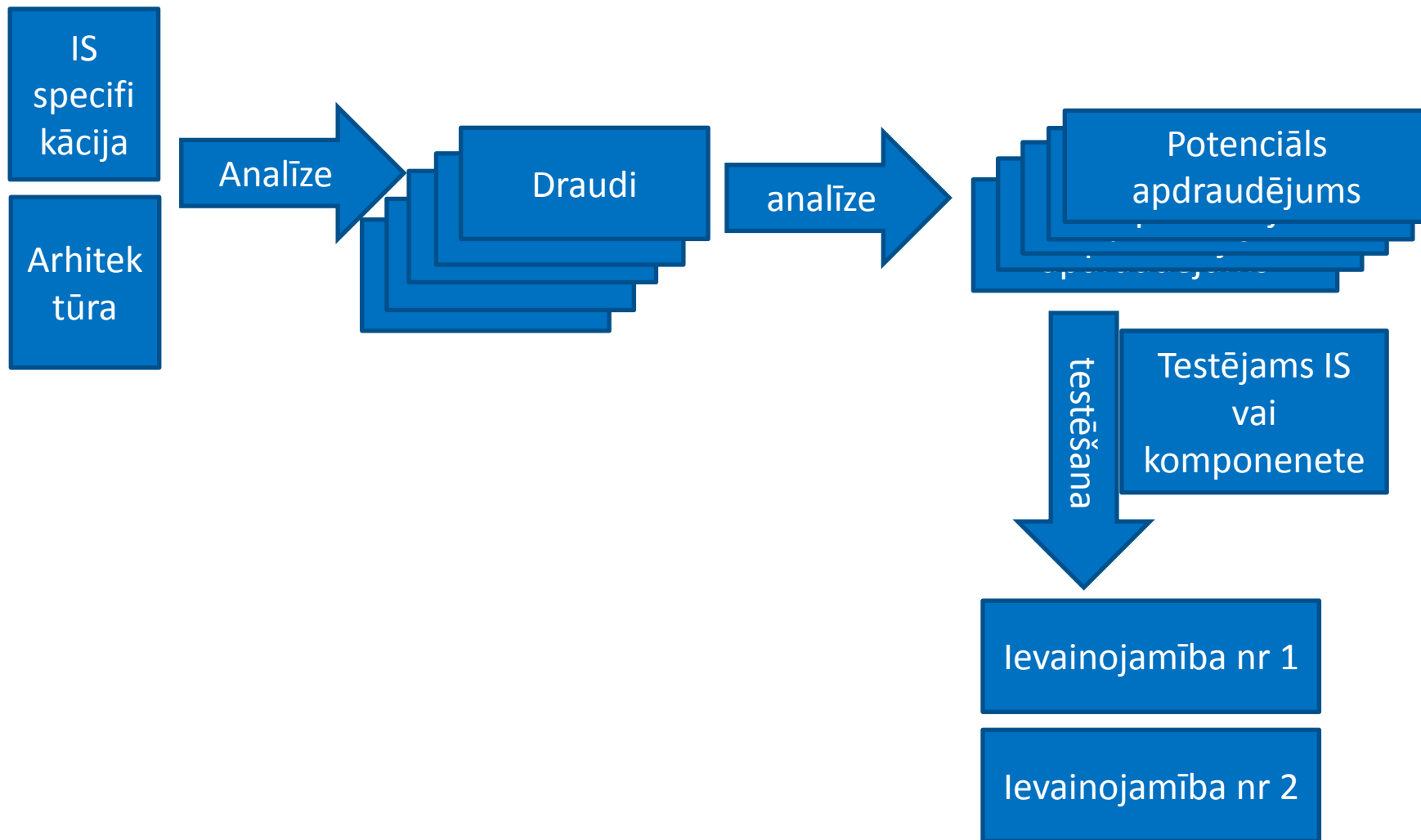
Termini, kas lietoti drošības testēšanā

Termins	EN	Īsā definīcija	Skaidrojums
Apdraudējums	Threat	Darbība vai notikums, kas var novest pie nesankcionētas piekļuves ... bojājumiem, traucējumiem...	Identificēts uzlaušanas scenārijs
Draudi	Threat	Notikums, kas apdraud organizāciju	Īstenota apdraudējuma sekas
Ievainojamība	Vulnerability	IS nepilnība, kas ļauj apdraudējumam īstenoties	Caurums sistēmā, kas ļauj to uzlauzt
Nepilnība	Vulnerability	Jebkāda nepilnība, kas <i>var</i> sekmēt apdraudējumu	Caurums sistēmā, kas gan nerada tiešus draudus

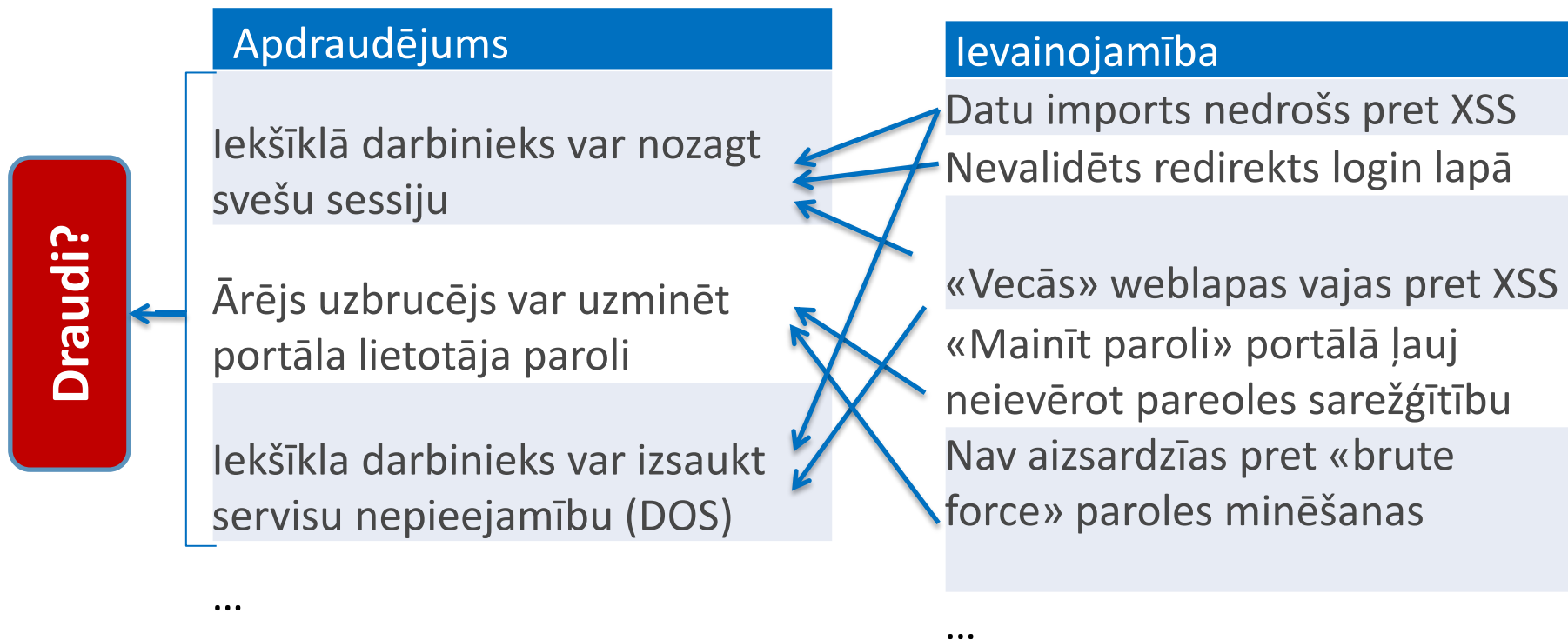
Tipiska testēšana audita ietvaros: Black-Box



Testēšana izstrādes laikā



Apraudējumu rada ievainojamība(s)



Drošības pasākumu pārskats: Apdraudējumu klases

- Aplikācijas draudu klasifikācija:
 - Izlikšanās (Spoofing identity)
 - Datu manipulācijas (Tampering with data)
 - Noliegums (Repudiation)
 - Informācijas atklāšana (Information disclosure)
 - Pakalpojumu nepieejamība (Denial of service)
 - Privilēģiju pārsniegšana (Elevation of privilege)
- Avoti:
 - OWASP: Application threat model
 - MSDL: The STRIDE Threat Model

Draudu veidu pārklājums izstrādes dzīvescilā

	Prasības	Dizains	Izstrāde	Testi
Izlikšanās	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Datu manipulācijas	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Noliegums	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Informācijas atklāšana	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
Servisa nepieejamība	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Privilēģiju pārsniegšana	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>

Secinājumi

- Problēma: kā atšķirt drošu programmu no nedrošas?
- Audits
 - Kā nodrošināt pilnu, kvalificētu auditu?
 - Ārējais audits nespēj atrisināt visas problēmas (laicīgi)
- Izstrādātāja metodoloģija
 - Vai metodoloģiju var izvērtēt? Ko tā nodrošina?
- Līgums par pakalpojumu līmeni (SLA)
 - Drošības prasības, drošības pasākumu prasības, nodevumi
 - Drošības problēmu sankcijas

JAUTĀJUMI?

Kontakti:

Ainārs Galvāns

Risinājumu drošības speciālists, Exigen Services Latvia

ainars.galvans@exigenservices.com

Eizensteina iela 29a | Rīga, LV-1079, Latvia

phone +371 6707 2976 | mobile +371 2943 2698

www.exigenservices.lv