



Haavoittuvuudet kuriin

Oskari Forsblom

COALA

Sisällysluettelo ja johdanto

- Coalasta ja allekirjoittaneesta muutama sananen
- Yleistä haavoittuvuuksista
- Oikean elämän esimerkki
- Esimerkki haavoittuvasta sovelluksesta
 - Haavoittuvan sovelluksen tarkastelu
 - Demo
- Arkkitehtuuri ja Katakri
- Yhteenveto

Coala Oy



Perustettu 2011



Työntekijöitä 8



Liikevaihto >600 k€



Kasvuyritys



Sijainti Helsinki



Konsultointi ja koulutus



Yksityisesti omistettu

Palvelumme: Konsultointia ja koulutusta



Kokonaisarkkitehtuuritoiminnon pystytys



Ratkaisuarkkitehtuurit



Kokonaisarkkitehtuurin haltuunotto



Prosessien kehittäminen



Arkkitehtuuri jatkuvana palveluna



Käyttäjähallinnan (IAM) arkkitehtuurit



Arkkitehti resurssina



Kehittämisen työtapojen ohjeistus



Välinevalinnan tuki



Avoimet koulutukset



Välineen käyttöönotto



Webinaarit



Välineen haltuunotto



Valmennusohjelmat



Kypsyystasoarvio, Osaamiskartoitus



Asiakaskohtaiset koulutukset



OSKARI FORSBLOM

TEKNOLOGIA-ARKKITEHTI
SEKÄ TIETOTURVAN JA
SOVELLUSKEHITYKSEN
TAITAJA

KUKA OLEN

Olen teknologioista kiinnostunut IT -alan ammattilainen, joka on uransa aikana ollut mukana sovelluskehityksessä, tietoliikennehommissa sekä elektroniikan suunnittelussa. Viimeiset vuodet olen keskittynyt teknologia-arkkitehtuuriin sekä tietoturvaan. Vapaa-ajalla puuhastelen omien sovelluskehitysprojektien parissa

YHTEYSTIEDOT

☎ (358) 50 4523843

✉ oskari.forsblom@coala.fi

SOSIAALINEN MEDIA

in <https://www.linkedin.com/in/oskari-forsblom-67669ab8/>

github <https://github.com/oskarifo/>

COALA

Jos esitys miellytti, niin käykää ihmeessä verkostoitumassa kanssani

27.5.2021

TYÖKOKEMUS

COALA

2021->

LIIKENNE JA VIESTINTÄVIRASTO TRAFICOM

2019-2021

LIIKENTEEN TURVALLISUUSVIRASTO TRAFI

2014-2018

PUOLUSTUSVOIMAT

2013

ARCTEQ

2012

KOULUTUS

Vaasan ammattikorkeakoulu,
Tietotekniikan insinööri

HARRASTUKSET

KOODAUS

- Perheelle "tarpeellisten" sovellusten väsäminen
- Pelien väsäminen
- IoT -laitteet

VALOKUVAUS

VINYYLIEN KERÄILY JA KUUNTELU

KAHVI

LENKKEILY

Haavoittuvuudet kuriin

5

HAAVOITTUVUUDET

Mikä on haavoittuvuus?

- "A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety).“ CVE Mitre
- *CVE Common Vulnerabilities and Exposures, yleinen haavoittuvuus ja altistuminen*

Raportointi

- Maailmalla:
 - [CVE - Home \(mitre.org\)](https://www.mitre.org/cve)
 - [NVD - Vulnerabilities \(nist.gov\)](https://nvd.nist.gov)
 - [Vulnerability Database !\[\]\(cd3e54d951a9fb854f48e4697cf550f9_img.jpg\) \(vuldb.com\)](https://vuldb.com)
- Tuotevalmistajat:
 - [Security Bulletins - Red Hat Customer Portal](#)
 - [Vulnerabilities - Security Update Guide - Microsoft](#)
- Suomessa:
 - [CERT | Kyberturvallisuuskeskus](#)
 - *mm. Sähköpostijakelu, RSS -syöte*

Miten yleisiä haavoittuvuuksia luokitellaan

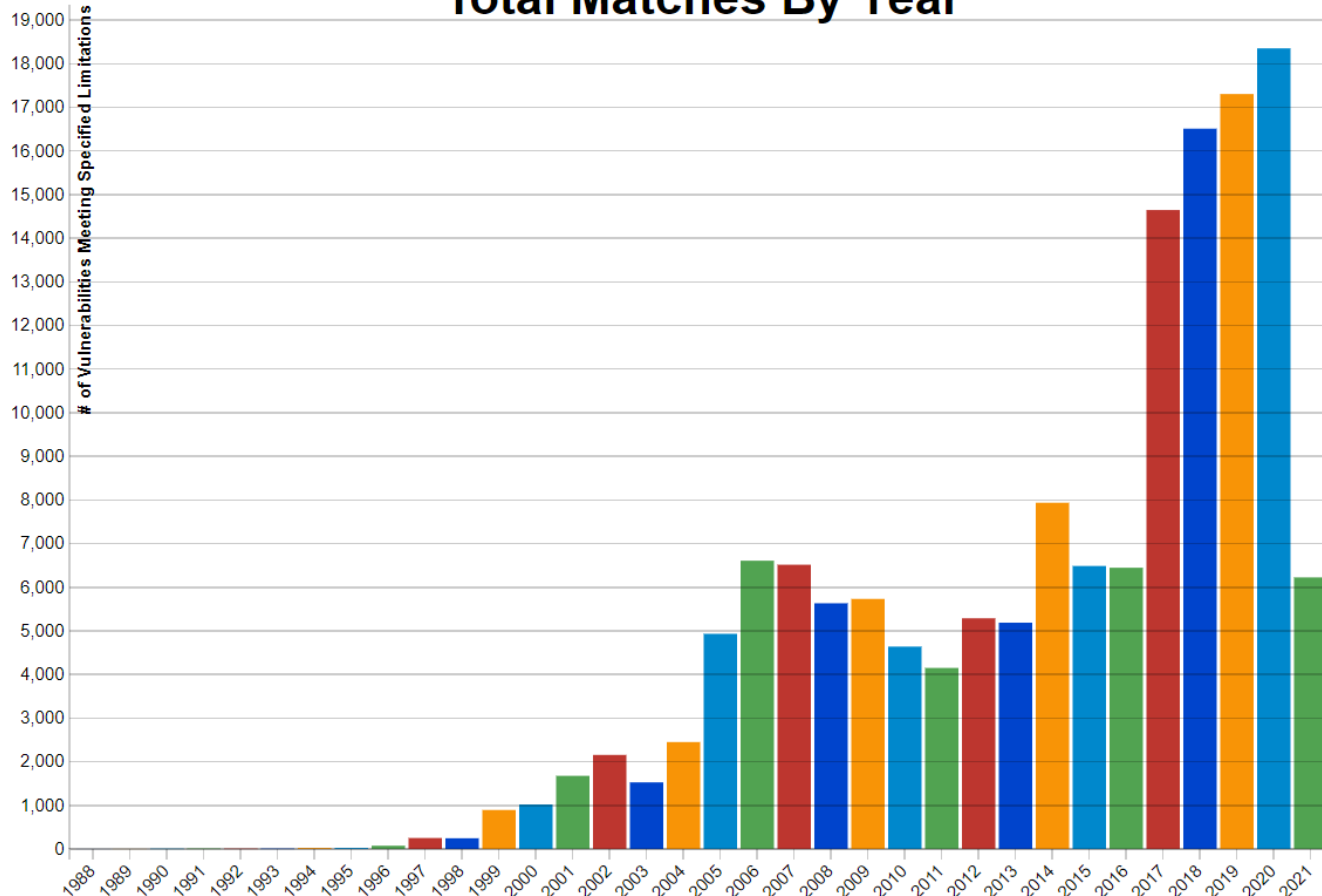
- Haavoittuvuudet luokitellaan The Common Vulnerability Scoring System (CVSS) järjestelmän avulla asteikolla on 0 – 10
- The National Vulnerability Database (NVD) tarjoaa CVSS pisteytykset lähes kaikille yleisille haavoittuvuuksille
- CVSS:stä on käytössä kaksi eri versiota v2 sekä v3

CVSS v2.0 Ratings	
Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings	
Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

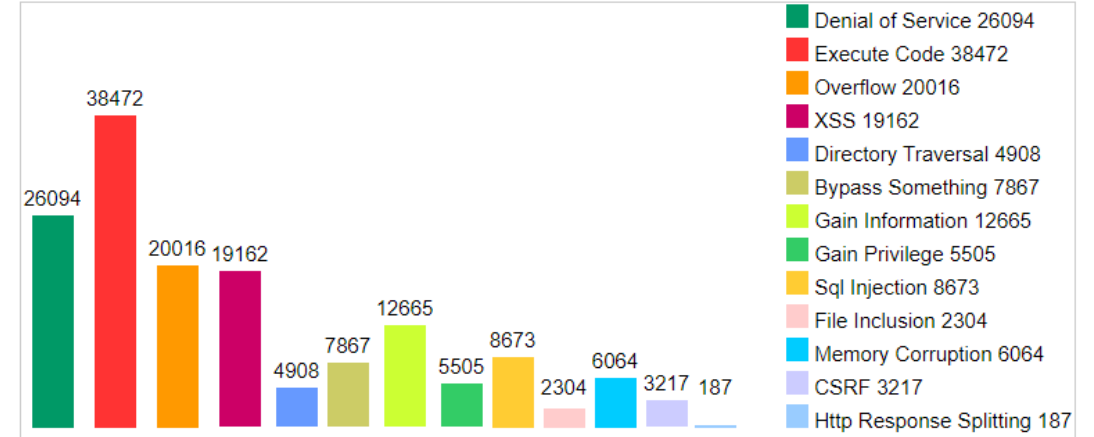
CVE - Haavoittuvuuksien kehitys

Total Matches By Year



Lähde: <https://nvd.nist.gov>

Vulnerabilities By Type



Lähde: [Vulnerability distribution of cve security vulnerabilities by types \(cvedetails.com\)](https://cvedetails.com)

CWE – Common Weakness Enumeration

1350 - Weaknesses in the 2020 CWE Top 25 Most Dangerous Software Weaknesses

- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') - (79)
- Out-of-bounds Write - (787)
- Improper Input Validation - (20)
- Out-of-bounds Read - (125)
- Improper Restriction of Operations within the Bounds of a Memory Buffer - (119)
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') - (89)
- Exposure of Sensitive Information to an Unauthorized Actor - (200)
- Use After Free - (416)
- Cross-Site Request Forgery (CSRF) - (352)
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') - (78)
- Integer Overflow or Wraparound - (190)
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') - (22)
- NULL Pointer Dereference - (476)
- Improper Authentication - (287)
- Unrestricted Upload of File with Dangerous Type - (434)
- Incorrect Permission Assignment for Critical Resource - (732)
- Improper Control of Generation of Code ('Code Injection') - (94)
- Insufficiently Protected Credentials - (522)
- Improper Restriction of XML External Entity Reference - (611)
- Use of Hard-coded Credentials - (798)
- Deserialization of Untrusted Data - (502)
- Improper Privilege Management - (269)
- Uncontrolled Resource Consumption - (400)
- Missing Authentication for Critical Function - (306)

Class - a weakness that is described in a very abstract fashion, typically independent of any specific language or technology. More specific than a Pillar Weakness, but more general than a Base Weakness. Class level weaknesses typically describe issues in terms of 1 or 2 of the following dimensions: behavior, property, and resource.

- Haavoittuvuudet johtuvat jostain heikkoudesta sovelluksessa tai raudassa, jota väärinkäyttämällä saa aikaiseksi negatiivisen vaikutuksen lopputulokseen
- Yleiset haavoittuvuudet määritetään CWE määritysten mukaisiin heikkouksiin

Lähde: "2020 CWE Top 25 Most Dangerous Software Weaknesses". 2020-08-20.
<http://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html>.

OIKEAN ELÄMÄN ESIMERKKI

Luottotietoyhtiö Equifax tietomurto vuonna 2017

- 147 miljoonan henkilön tiedot vuosivat
 - mm. Nimitiedot, henkilötunnukset, syntymäajat, luottokortin numerot
- Haavoittuvuus avoimen lähdekoodin sovelluskehityksessä (Apache Struts)
 - [NVD - CVE-2017-5638 \(nist.gov\)](https://nvd.nist.gov/vuln/detail/CVE-2017-5638)

ESIMERKKI HAAVOITTUVUUKSISTA

Sovellukset

- Esimerkkijärjestelmä koostuu hyvin perinteisestä teknologiasta
 - Järjestelmän rakenne jakautuu kahteen osaan; käyttöliittymään sekä taustaan
- Järjestelmässä on esimerkin vuoksi käytössä vanhentuneita versiota kirjastoriippuvuuksista. (~5v vanhoja)

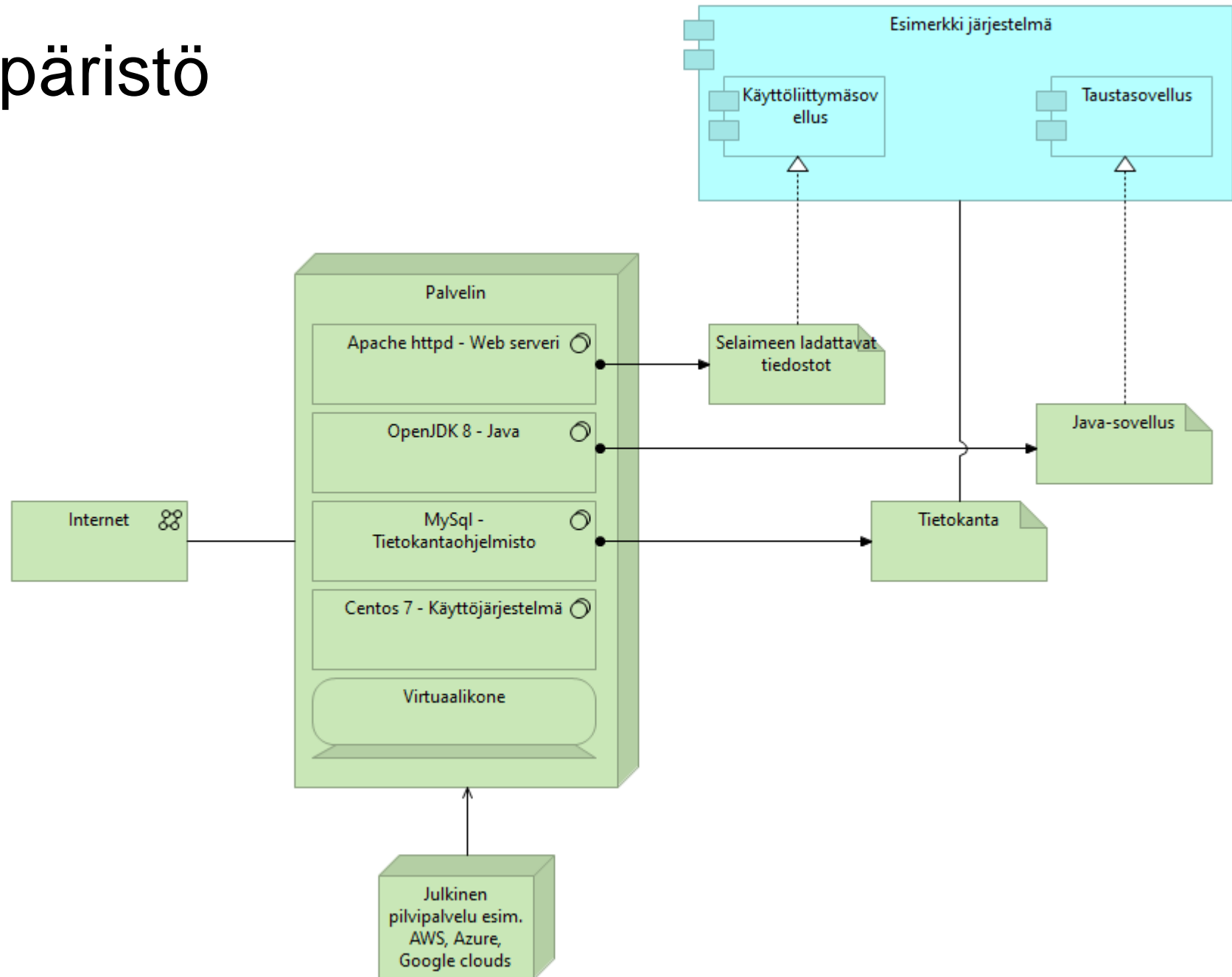
Käyttöliittymäsovellus (selainsovellus):

- **Vue.js (Javascript)**
 - Hyvin yleinen sovelluskehys käyttöliittymäsovelluksille

Tausta sovellus (serverisovellus):

- **Spring Boot (Java)**
 - Hyvin yleinen sovelluskehys taustajärjestelmien toteutukseen

Palvelinympäristö



Potentiaalisia hyökkäysvektoreita

- Järjestelmässä auki Internetiin komponentteja, joiden ei tarvitsisi olla suoraan kutsuttavissa Internetistä
- Järjestelmässä paljon vanhentuneita komponentteja, jotka voivat pitää sisällään haavoittuvuuksia
- Järjestelmän kaikki komponentit pyörivät samassa paikassa
- Liikennettä ei suodateta lainkaan ennen sen käsittelyä

DEMO

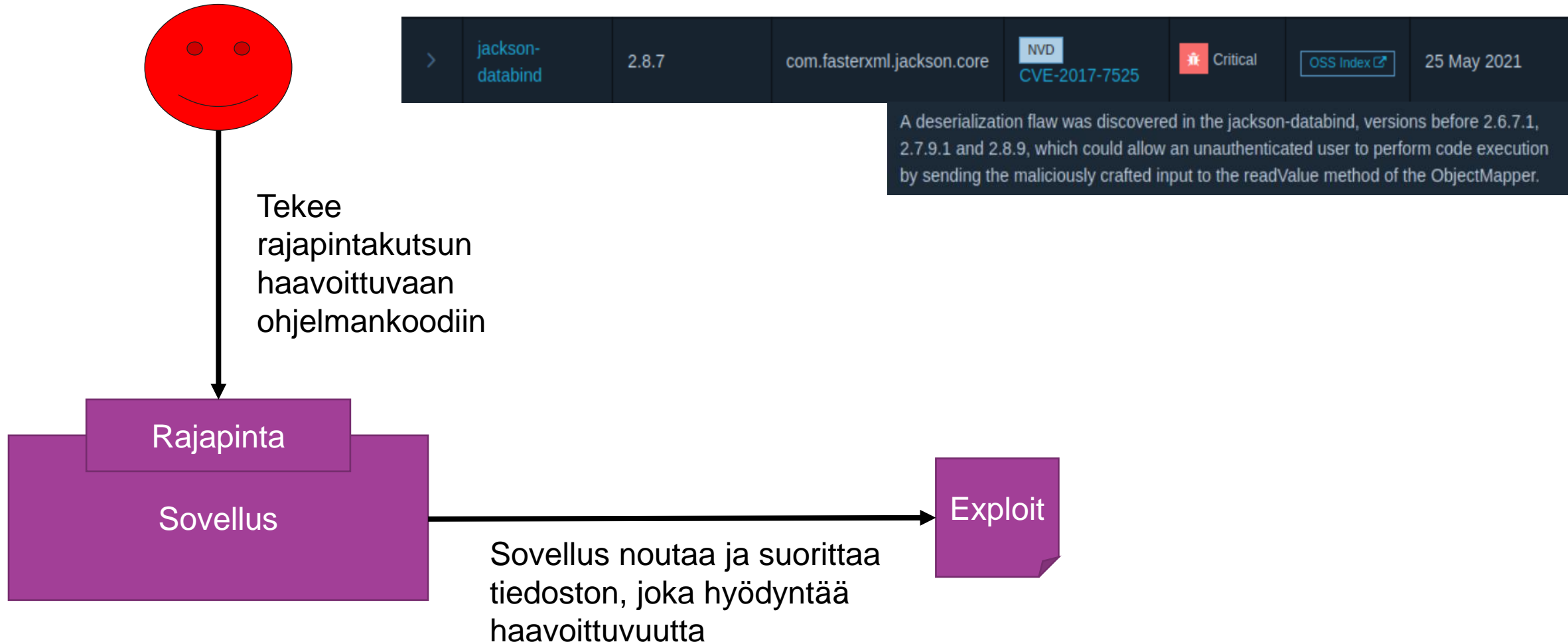
COALA

Dependency-Track

Project Name	Version	Last BOM Import	BOM Format	Risk Score	Active	Vulnerabilities
KAOS demo Backend	1.0	25 May 2021 at 16:02:48	CycloneDX 1.2	520	<input checked="" type="checkbox"/>	31 29 20
KAOS demo Frontend	1.0	25 May 2021 at 15:49:54	CycloneDX 1.2	113	<input checked="" type="checkbox"/>	2 14 6 5

	Component	Version	Group	Vulnerability	Severity	Analyzer	Attributed On	Analysis	Suppressed
>	spring-data-commons	1.13.1.RELEASE	org.springframework.data	NVD CVE-2018-1273	✘ Critical	OSS Index	25 May 2021		
>	tomcat-embed-core	8.5.11	org.apache.tomcat.embed	NVD CVE-2020-1938	✘ Critical	OSS Index	25 May 2021		
>	tomcat-embed-core	8.5.11	org.apache.tomcat.embed	NVD CVE-2018-8014	✘ Critical	OSS Index	25 May 2021		
>	jackson-databind	2.8.7	com.fasterxml.jackson.core	NVD CVE-2017-7525	✘ Critical	OSS Index	25 May 2021		

Haavoittuvuus



Haavoittuvuus käytännössä

1. Haavoittuvan sovelluksen ajoympäristö ennen haavoittuvuuden hyödyntämistä.

3. Hyökkääjä saa haavoittuvan sovelluksen ajoympäristön suorittamaan hyökkääjän määrittämää koodia

2. Hyökkääjä kutsuu haavoittuvaa rajapintaa

POST http://localhost:8082/

Send

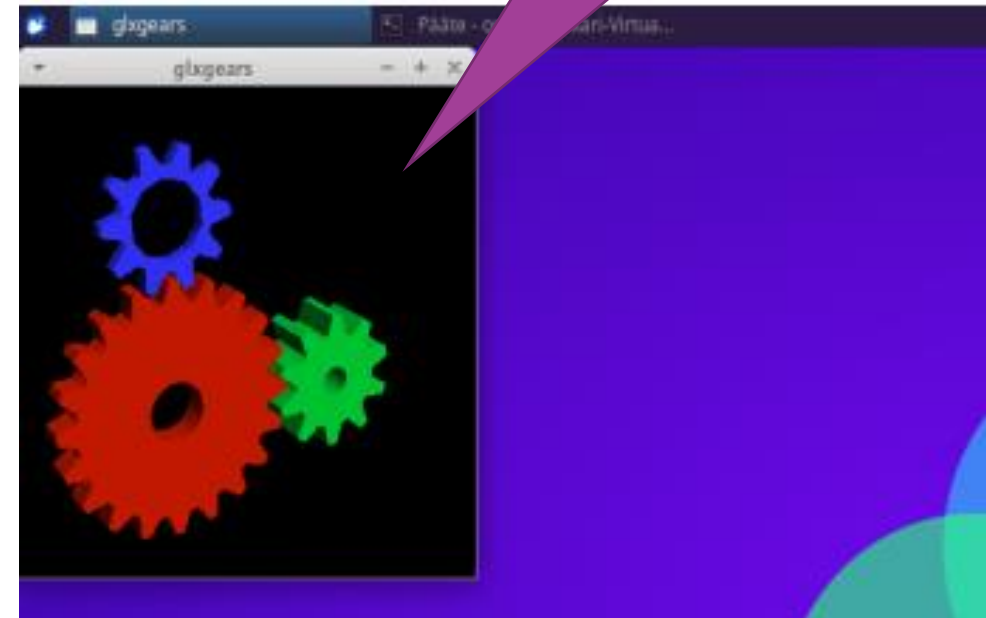
JSON

Auth

Query

Header 1

Docs



Työkaluja

- Haavoittuvuuksien tunnistamiseen on olemassa useita eri työvälineitä sekä menetelmiä, alla joitain esimerkkejä työkaluista
 - Skannaustyökalut ja Penetraatiotyökalut
 - OWASP® Zed Attack Proxy (ZAP)
 - Burb Suite
 - Nmap
 - Ja lukuisia muita
 - **Analystointityökalut**
 - Dependency Track
 - Dependency Check
 - SonarQube Security Analysis
 - CI/CD työkalut (Github, Gitlab)
 - Ja lukuisia muita

KATAKRI 2020

Katakri

- Katakri on viranomaisten tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset.
- Ensimmäinen Katakri eli kansallinen turvallisuusauditointikriteeristö valmistui vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa.
- Katakriin neljännen version päivitystyön taustalla keskeisimpänä tekijänä on ollut vastaaminen 2020 alusta uusiutuneen kansallisen lainsäädännön muutoksiin. Neljännessä versiossa on huomioitu myös digitaalisen tietojenkäsittelyn kehitysaskelleita, sekä täydennetty työkalun tarkoituksenmukaiseen käyttöön liittyviä ohjeistuksia

Katakriin rakenne

- Katakriin on jaettu kolmeen osa-alueeseen.
 - Turvallisuusjohtamista koskevassa (T) osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä sekä riittävät henkilöstöturvallisuuden menettelyt turvallisuusluokiteltujen tietojen suojaamiseen.
 - Fyysistä turvallisuutta koskevassa (F) osa-alueessa kuvataan turvallisuusluokiteltujen tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset.
 - Teknistä tietoturvallisuutta koskevassa (I) osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset.
- Vaatimukset on kuvattu siten, että ne mahdollistavat erilaisia toteutustapoja. Lisätietokenttiin on tulkinnan tueksi koottu toteutusesimerkkejä, joissa kuvatuilla menettelyillä voidaan useimmissa ympäristöissä saavuttaa hyväksyttävä suojausten vähimmäistaso. Toteutusesimerkit eivät ole sitovia ja ne ovat korvattavissa myös muilla vastaavan tasoilla suojauksilla

Esimerkki vaatimuksesta.

I-19 TIETOJENKÄSITTELY-YMPÄRISTÖN SUOJAUS KOKO ELINKAAREN AJAN – OHJELMISTOHAAVOITUVUUKSIEN HALLINTA

Vaatus

§ Lähde (906/2019 ja/tai 1101/2019)

§ Lähde (2013/488/EU)

Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.

906/2019 13 §

IV liitteen 8, 11 ja 16 kohdat

Lisätietoja

Yleistä: Ohjelmistovirheiden, toisin sanoen haavoittuvuuksien, hyödyntäminen on useissa hyökkäystyypeissä jossain vaiheessa mukana. On huomioitava, että haavoittuvaa lähdekoodia on niin käyttöjärjestelmäohjelmistoissa, palvelinsovelluksissa, loppukäyttäjäsovelluksissa, kuin esimerkiksi laiteohjelmistotason (firmware) sovelluksissa ja ajureissa, BIOS:issa ja erillisissä hallintaliittymissä (esim. iLo, iDrac). Ohjelmistovirheiden lisäksi haavoittuvuuksia aiheuttaa konfiguraatiovirheistä ja vanhoista käytänteistä, esimerkiksi vanhentuneiden salausalgoritmien käytöstä. Vastuulliset toimittajat korjaavat ohjelmistoistaan löytyneitä haavoittuvuuksia. Riskejä voidaan pienentää korjausten asennuksilla. Haavoittuvuuden hallintaa toteuttaessa tulee huolehtia haavoittuvuusskannerin, CMDB:n ja muiden järjestelmien ajantasaisuudesta ja tietoturvallisuudesta.

Haavoittuvuuksien hallinnan tulisi tähdätä tarkan tilannekuvan muodostamiseen siten, että toimintaan liittyy ohjelmisto- ja järjestelmäympäristön jatkuva seuranta ja kehittäminen. Osana tilannekuvan ylläpitoa havaittujen puutteiden ja erilaisten haavoittuvuuksien aiheuttama riski tulisi arvioida suhteessa käyttöympäristöön ja asettaa korjaavat toimenpiteet perustuen tämän arvion kriittisyyteen. Korjaavia toimenpiteitä ovat mm. ohjelmistotoimittajien haavoittuvuuskorjaukset, päivitykset ja konfiguraatiomuutokset, jotka tähtäävät riskin poistamiseen tai rajaamiseen. Lisäksi on syytä seurata käytettävien ohjelmistoversioiden tukea niiden toimittajalta. Vanhentuneisiin ohjelmistoversioihin ei julkaista aktiivisesti päivityksiä, jolloin myös tietoturva- ja haavoittuvuuksien korjaaminen voi olla mahdotonta. Tehokas prosessimainen haavoittuvuuksien hallinta edellyttää organisoitua ja vastuutettua toimintamallia, sekä yleensä myös organisaation sisäisten ja ulkoisten sidosryhmien yhteistyötä.

Ohjelmistohaavoittuvuuksien hallintaa voidaan toteuttaa esimerkiksi siten, että

1. Sähköpostiin on tilattu CERT-toimijoiden sekä valmistajien tiedotukset. Tiedotuksista poimitaan sellaiset, jotka vaikuttavat organisaation järjestelmien turvallisuuteen. Poiminnan mahdollistamiseksi on olemassa ajantasainen järjestelmäkirjanpito ohjelmistojen ja näiden versioiden osalta (ks. järjestelmäkirjanpito kohdasta I-16). Ladattujen ohjelmistojen ja päivitysten eheys tarkistetaan (tarkistussummat, haittaohjelmataarkistus) ennen niiden jakamista tuotantoympäristöön. Päivitysten vaikutukset tulisi mahdollisuuksien mukaan testata ennen tuotantoympäristöön asennusta. Testaus voidaan suorittaa esimerkiksi eristetyssä testiympäristössä tai pienellä käyttäjäjoukolla.
2. Päivitysten asentamisen onnistumista tarkastellaan säännöllisesti, vähintään kuukausittain. Tarkasteluun voidaan hyödyntää esimerkiksi keskittyjä päivityksenjako- ja -hallintapalveluita tai vastaavia menettelyjä.
3. Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet, tulostimet, mobiililaitteet ja vastaavat tarkastetaan kattavasti (haavoittuvuusskannaus, CMDB jne.) säännöllisesti ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi.

Osa-alue I: Tekninen tietoturvallisuus

- Kataktrin teknisen tietoturvallisuuden osa-alueessa kuvataan vaatimukset, joita soveltamalla pyritään varmistamaan turvallisuusjärjestelyjen riittävyys viranomaisen turvallisuusluokitellun tiedon sähköisissä käyttöympäristöissä.
- Vaatimukset on jaettu tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuuden osioihin. Tiettyihin asiakokonaisuuksiin (esimerkiksi hallintayhteydet, langattomat verkot, etäkäyttö ja varmuuskopiointi) on ryhmitelty niihin liittyvät vaatimukset

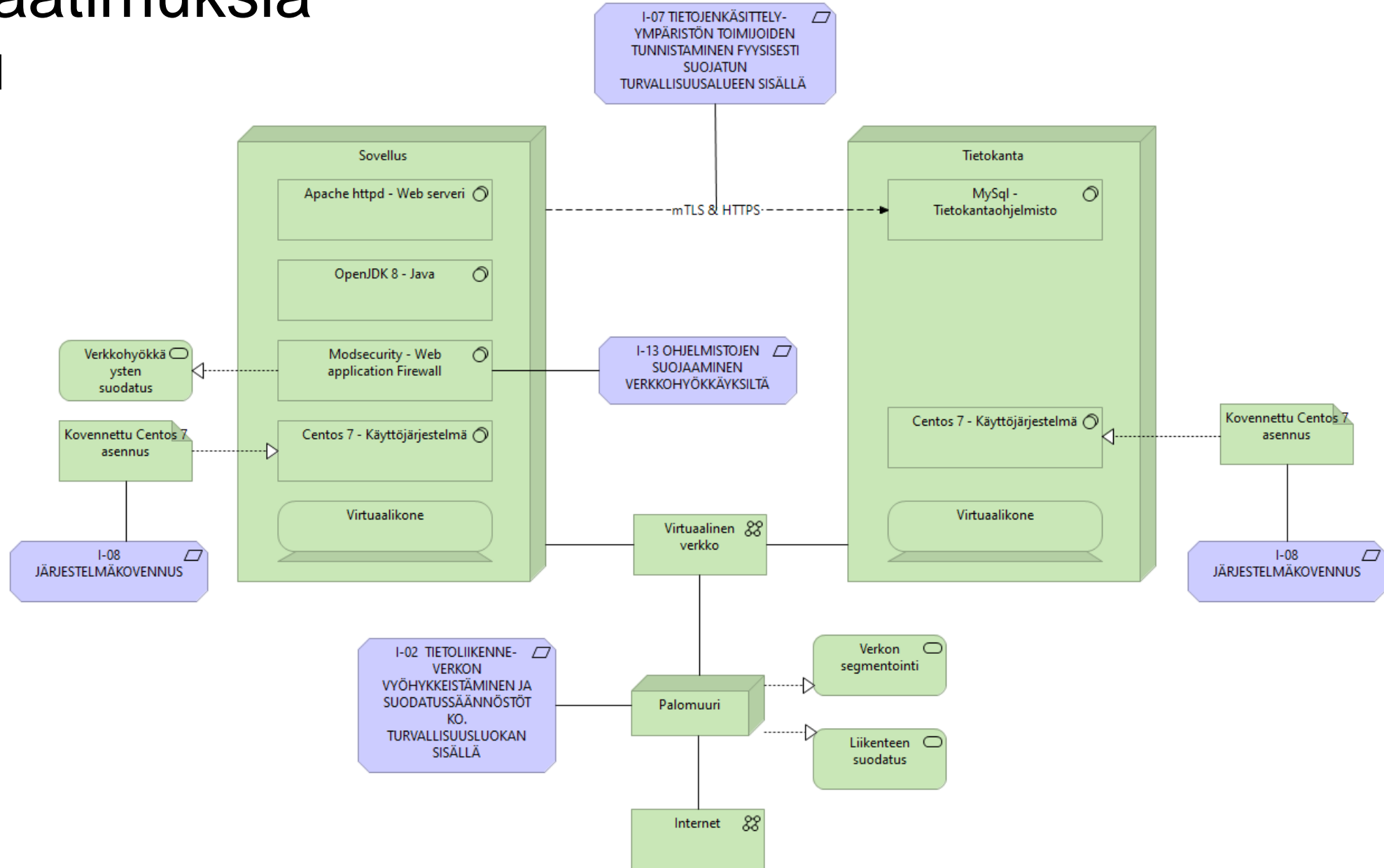
Katakri 2020

- I-01 TIETOJENKÄSITTELY-YMPÄRISTÖJEN SUOJATTU YHTEENLIITTÄMINEN – VERKON RAKENTEELLINEN TURVALLISUUS
- **I-02 VÄHIMPIEN OIKEUKSIEN PERIAATE - TIETOLIIKENNE-VERKON VYÖHYKKEISTÄMINEN JA SUODATUSÄÄNNÖSTÖT KO. TURVALLISUUSLUOKAN SISÄLLÄ**
- I-03 TIETOJENKÄSITTELY-YMPÄRISTÖN TURVALLISUUS KOKO ELINKAAREN AJAN – SUODATUS- JA VALVONTAJÄRJESTELMIEN HALLINNOINTI
- I-04 TIETOJENKÄSITTELY-YMPÄRISTÖJEN SUOJATTU YHTEENLIITTÄMINEN – HALLINTAYHTEYDET
- I-05 SUOJATTAVIEN TIETOJEN SIIRTÄMINEN FYYSISESTI SUOJATTUJEN ALUEIDEN ULKOPUOLELLA - LANGATON TIEDONSIIRTO
- I-06 VÄHIMPIEN OIKEUKSIEN PERIAATE – PÄÄSYOIKEUKSIEN HALLINNOINTI
- **I-07 MONITASOINEN SUOJAAMINEN – TIETOJENKÄSITTELY-YMPÄRISTÖN TOIMIJOIDEN TUNNISTAMINEN FYYSISESTI SUOJATUN TURVALLISUUSALUEEN SISÄLLÄ**
- **I-08 VÄHIMMÄISTOIMINTOJEN JA VÄHIMPIEN OIKEUKSIEN PERIAATE – JÄRJESTELMÄKOVENNUS**
- **I-09 MONITASOINEN SUOJAAMINEN – HAITTAOHJELMASUOJAUS**
- I-10 MONITASOINEN SUOJAAMINEN – TURVALLISUUTEEN LIITTYVIEN TAPAHTUMIEN JÄLJITETTÄVYYS
- I-11 MONITASOINEN SUOJAAMINEN – POIKKEAMIEN HAVAINNOINTIKYKY JA TOIPUMINEN

Katakri 2020

- I-12 TIETOTURVALLISUUSTUOTTEIDEN ARVIOINTI JA HYVÄKSYNTÄ – SALAUSRATKAISUT
- **I-13 MONITASOINEN SUOJAAMINEN KOKO ELINKAAREN AJAN – OHJELMISTOJEN SUOJAAMINEN VERKKOHYÖKKÄYKSILTÄ**
- I-14 MONITASOINEN SUOJAAMINEN – HAJASÄTEILY (TEMPEST) JA ELEKTRONINEN TIEDUSTELU
- I-15 TURVALLISUUSLUOKITELTUIEN TIETOJEN VÄLITYS FYYSISESTI SUOJATTUIEN ALUEIDEN VÄLILLÄ – TIEDON SÄHKÖINEN VÄLITYS
- **I-16 TURVALLISUUSLUOKITELLUN TIEDON KÄSITTELYYN LIITTYVÄN TIETOJENKÄSITTELY-YMPÄRISTÖN SUOJAUS KOKO ELINKAAREN AJAN – MUUTOSHALLINTAMENETTELYT**
- I-17 TURVALLISUUSLUOKITELTUIEN SÄHKÖISESSÄ MUODOSSA OLEVIER TIETOJEN KÄSITTELY FYYSISESTI SUOJATTUIEN ALUEIDEN SISÄLLÄ - FYYSINEN TURVALLISUUS
- I-18 TURVALLISUUSLUOKITELTUIEN TIETOJEN VÄLITYS JA KÄSITTELY FYYSISESTI SUOJATTUIEN ALUEIDEN VÄLILLÄ - ETÄKÄYTTÖ JA ETÄHALLINTA
- **I-19 TIETOJENKÄSITTELY-YMPÄRISTÖN SUOJAUS KOKO ELINKAAREN AJAN – OHJELMISTOHAAVOITTUVUUKSIEN HALLINTA**
- I-20 TIETOJENKÄSITTELY-YMPÄRISTÖN SUOJAUS KOKO ELINKAAREN AJAN – VARMUUSKOPIOINTI
- I-21 TIETOJENKÄSITTELY-YMPÄRISTÖN SUOJAUS KOKO ELINKAAREN AJAN – SÄHKÖISESSÄ MUODOSSA OLEVIER TURVALLISUUSLUOKITELTUIEN TIETOJEN TUHOAMINEN

Katakrin vaatimuksia huomioutu



Miten hyökkäysvektoria on piennetty

- Palvelut eivät ole enää suoraan kutsuttavissa turvattomista verkoista
 - Palomuuuri suodattaa pois kaikki muut protokollat kuin sallitut
 - Palomuuuri suodattaa pois kutsut muihin portteihin kuin tarvittaviin
 - Palomuuuri sallii/estää yhteysavaukset
 - Inbound, mistä kutsut sallitaan
 - Outbound, mihin palvelu voi ottaa yhteyttä
- Verkkohyökkäysten suodatus
 - Modsecurity (Web application firewall) estää tunnettuja hyökkäyksiä mm. xss, injectiot jne...
- Komponentit tunnistetaan
 - Tietojärjestelmän komponentit tunnistavat toisensa ja sallivat vain kutsut niiltä tahoilta, joille annettu oikeus tehdä kutsuja
- Kovennukset
 - Palvelimella on vain ja ainoastaan pakolliset ohjelmistot asennettuina
 - Palvelimella on käyttöoikeudet määritelty vähimpien oikeuksien periaatteella, myös prosessit ja järjestelmät
 - Palvelimella on audit -lokitus päällä

YHTEENVETO

Yhteenveto

- Tietojärjestelmien haavoittuvuuksia tulee seurata
- Katakria voi käyttää muuhunkin kuin vain auditointityökaluksi
- Hyvin suunniteltu arkkitehtuuri pienentää hyökkäysvektoria
- Tietoturva on riskiperusteista
- Yleisten haavoittuvuuksien seuraaminen ja korjaaminen ei yksinään riitä

