**1 Tim za odgovor na incidente naziva se**

Computer System Incident Response Team (CSIRT)

Information Systems Incident Response Team (ISIRT)

Information Security Emergency Team (ISET)

Computer Emergency Team (CET)

Computer Security Incident Response Team (CSIRT) <--

**2 Kratica SRIDE označava praksu modeliranja prijetnji, koja podrazumijeva**

Spoofing, Threatening, Repudiation, Information, Denial, Elevation

Spoofing, Tampering, Reproducibility, Information, Denial, Elevation

Spoofing, Tampering, Repudiation, Information, Damage, Elevation

Spoofing, Tampering, Repudiation, Information, Discoverability, Elevation

Spoofing, Tampering, Repudiation, Information, Denial, Elevation <--

**3 U praksi STRIDE, Denial of Service ukazuje na prijetnje s obzirom na**

This question contains multiple correct answers!

Spremišta podataka

Sudionike

Sve navedeno

Tokove podataka <--

**4 Procedure za prelazak s primarne na pričuvnu lokaciju i obrnuto su**

Backover, Switchback

Failover, Switchback

Backup, Restore, Rollforward

Failover, Switchover, Failback <--

Switching, Recovery

**5 Koje su prakse faze Verification u SSDLC**

This question contains multiple correct answers! <--

Threat Model and Attack Surface Review <--

Fuzz Testing

Incident Response Plan

Final Review

Dynamic Program Analysis <--

**6 U praksi STRIDE, Spoofing ukazuje na prijetnje s obzirom na**

This question contains multiple correct answers!

Procese

Sudionike

Sve navedeno <--

Tokove podataka

Spremišta podataka

**7 Prakse smanjenja površine napada su**

This question contains multiple correct answers!

Redukcija privilegija <--

Redukcija kôda koji se izvodi prema zadanim postavkama (by default) <--

Ograničenje pristupa nepouzdanim korisnicima <--

Instalacija antivirusne zaštite

Kontrola rizika

**8 Sigurnosni zahtjevi su**

Korisnički zahtjevi

Nefunkcionalni zahtjevi

Funkcionalni zahtjevi

Posebna vrsta zahtjeva

Poslovni zahtjevi

**9 Koraci inspekcije su**

Planiranje, Priprema, Sastanak, Prerada, Kontrola <---

Planiranje, Analiza, Provjera, Dorada, Dokumentiranje

Planiranje, Dizajn, Sastanak, Prerada, Revizija

Analiza, Dizajn, Konstrukcija, Integracija, Revizija

Planiranje, Priprema, Konstrukcija, Prerada, Revizija

**10 Odaberite modele životnog ciklusa sigurnog softvera**

This question contains multiple correct answers!

Rational Unified Process

Software Assurance Maturity Model

Trustworthy Computing Security Development Life Cycle

Scrum

Common Criteria

**11 Fuzzing (pročešljavanje) tehnika može biti (varijante)**

Lijepa ili pametna

Glupa ili pametna <---

Statička ili dinamička

Strukturirana ili objektna

Iterativna ili inkrementalna

**12 Koje su prakse faze Requirements u SSDLC**

This question contains multiple correct answers!

Quality Gates/Bug Bars <--

Design Requirements

Attack Surface Reduction

Security and Privacy Risk Assessment <--

Security Requirements <--

**13 Što od navedenog NIJE dio procesa modeliranja prijetnji**

Pregled arhitekture

Dokumentiranje prijetnji

Određivanje prijetnji

Određivanje sigurnosnih zahtjeva

Dekompozicija aplikacije

**14 Kriteriji početne točke penetracijskog testa mogu biti**

This question contains multiple correct answers!

Organizacijski

Tehnološki

Socijalni

Unutrašnji <--

Vanjski <---

**15 U praksi STRIDE, tokovi podatka ukazuju na prijetnje**

This question contains multiple correct answers!

Spoofing

Information Disclosure

Denial of Service

Repudiation

Tampering With Data

Elevation of Privilege

**16 Plan koji se bavi obnavljanjem poslovanja na pričuvnoj lokaciji je**

Plan upravljanja rizikom

Plan kontinuiteta poslovanja

Plan odgovora na incident

Plan oporavka od katastrofe

Plan za nepredviđene situacije

**17 Analiza mrlja (Taint Analysis) je tehnika**

Analize sigurnosnih zahtjeva

Penetracijskog testiranja

Inspekcije programskog kôda

Dinamičkog testiranja

Statičke analize programa <--

**18 U praksi STRIDE, Elevation of Privilege ukazuje na prijetnje s obzirom na**

Sve navedeno

Sudionike

procese <--

Tokove podataka

Spremišta podataka

**19 Pri modeliranju sigurnosnih zahtjeva koriste se**

This question contains multiple correct answers!

Threat Use Cases

Abuse Cases

Security Use Cases

Misuse Cases

Vulnerability Use Cases

**20 Plan koji se bavi obnavljanjem sustava na originalnoj lokaciji je**

Plan za nepredviđene situacije

Plan odgovora na incident

Plan kontinuiteta poslovanja

Plan oporavka od katastrofe <--

Plan upravljanja rizikom

**21 U praksi STRIDE, spremišta podataka ukazuju na prijetnje**

This question contains multiple correct answers!

Repudiation (kada je riječ o osjetljvim podacima)

Tampering With Data

Information Disclosure

Denial of Service

Spoofing

Elevation of Privilege

**22 Analiza utjecaja na poslovanje analizira**

Poslovne procese, aktivnosti i transakcije

Poslovne zahtjeve, Korisničke zahtjeve, Funkcionalne zahtjeve, Nefunkcionalne zahtjeve

Ništa od navedenog

Nužne funkcije, Potrebne funkcije, Poželjne funkcije, Neobavezne funkcije

Kritične funkcije, Bitne funkcije, Potrebne funkcije, Poželjne funkcije <---

**23 RACI matrica određuje**

Faze (Requirements, Analysis, Construction, Integration)

Ništa od navedenog

Stanja (Release, Archive, Construct, Implement)

Uloge (Responsible, Accountable, Consulted, Informed) <--

Svojstva (Robustness, Availability, Confidentiality, Integrity)

**24 Koje su prakse faze Implementation u SSDLC**

This question contains multiple correct answers!

Deprecate Unsafe Functions

Dynamic Program Analysis

Fuzz Testing

Static Analysis

Use Approved Tools

**25 Vremensku toleranciju gubitka podataka određuje zahtjev**

Ciljana točka oporavka (RPO) <--

Vrijeme oporavka rada (WRT)

Vrijeme izrade pričuvne kopije (BUT)

Ciljano vrijeme oporavka (RTO)

Maksimalno prihvatljivo vrijeme ispada (MTD)

**26 Analiza toka podataka (Data Flow Analysis) je tehnika**

Inspekcije programskog kôda

Modeliranja prijetnji

Dinamičkog testiranja

Penetracijskog testiranja

Statičke analize programa

**27 Maksimalno vrijeme za oporavak poslovne funkcije određuje zahtjev**

Ciljano vrijeme oporavka (RTO)

Maksimalno prihvatljivo vrijeme ispada (MTD)

Trajanje oporavka funkcije (FRD)

Ciljana točka oporavka (RPO)

Vrijeme oporavka rada (WRT)

**28 Vraćanje nakon osposobljavanja sustava na primarnoj lokaciji naziva se**

Switchover

Switchback

Backover

Failover

Failback <--

**29 DREAD je kratica za klasifikaciju prijetnji koja podrazumijeva**

Damage potential, Reproducibility, Elevation of Privilege, Affected users, Discoverability

Damage potential, Repudiation, Exploitability, Affected users, Discoverability

Denial of Service, Reproducibility, Exploitability, Affected users, Discoverability

Damage potential, Reproducibility, Exploitability, Affected users, Denial of Service

Damage potential, Reproducibility, Exploitability, Affected users, Discoverability <--

**30 Aktivnosti procjene rizika su**

This question contains multiple correct answers!

Planiranje upravljanja rizikom

Određivanje prioriteta rizika

Nadziranje, praćenje rizika

Razrješenje rizika

Identifikacija rizika

Analiza rizika

**31 Koraci penetracijskog testiranja su**

Istraživanje, Analiza, Upad, Dokumentiranje, Brisanje tragova

Istraživanje, Pokretanje, Analiza, Brisanje, Dokumentiranje

Skeniranje, Analiza, Dobivanje pristupa, Zadržavanje pristupa, Brisanje tragova

Istraživanje, Skeniranje, Dobivanje pristupa, Zadržavanje pristupa, Brisanje tragova <--

Analiza, Priprema, Prijetnja, Upad, Povlačenje

**32 Mjerenje površine napada provodi se**

Inspekcijom programskog kôda

Periodičkim mjerenjem avenija napada te usporedbom s osnovicom <--

Mjerenjem razlika između verzija istog proizvoda

Modeliranjem prijetnji

Integralom vektora napada pojedinih aplikacija

**33 Graf kontrole toka (Control Flow Graph) je tehnika**

Statičke analize programa

Dinamičkog testiranja

Penetracijskog testiranja

Inspekcije programskog kôda

Modeliranja prijetnji

**34 U praksi STRIDE, Tampering ukazuje na prijetnje s obzirom na**

This question contains multiple correct answers!

Tokove podataka

Sve navedeno

Spremišta podataka

Sudionike

**35 Statička analiza obuhvaća postupke**

This question contains multiple correct answers!

Traženje pogrešaka

Provjera tipova, provjera stila

Razumijevanje programa

Provjera svojstava

Verifikacija programa

**36 Glavne faze SSDLC su**

Analiza, Projektiranje, Konstrukcija, Integracija, Implementacija

Planiranje, Analiza, Oblikovanje, Izrada, Primjena

Ništa od navedenog

Zahtjevi, Dizajn, Implementacija, Verifikacija, Isporuka <--

Incepcija, Elaboracija, Konstrukcija, Tranzicija

**37 Postupci razrješenja rizika su:**

Izbjegavanje, Postavljanje prioriteta, Smanjenje, Prihvaćanje

Analiza, Preusmjeravanje / dijeljenje, Nadziranje, Prihvaćanje

Izbjegavanje, Preusmjeravanje / dijeljenje, Smanjenje, Prihvaćanje <--

Analiza, Nadziranje, Smanjenje, Prihvaćanje

Planiranje, Nadziranje, Smanjenje, Prihvaćanje

**38 Dekompozicija aplikacije pri modeliranju prijetnji obuhvaća**

This question contains multiple correct answers!

Izradu sigurnosnog profila

Određivanje granica povjerenja, tokova podataka, mjesta unosa i privilegiranog kôda

Oblikovanje poslovnih procesa

Modeliranje podataka

Reverzno inženjerstvo programa

Pregled arhitekture

**39 Analiza mrlja je tehnika**

Fuzz testiranja

Modeliranja prijetnji

Statičke analize <--

Analize rizika

Dinamičke analize

**40 Aktivnosti kontrole rizika su**

This question contains multiple correct answers!

Identifikacija rizika

Razrješenje rizika <--

Nadziranje, praćenje rizika <--

Određivanje prioriteta rizika

Analiza rizika

Planiranje upravljanja rizikom <--

**41 DREAD model procjenjuje rizik**

Sumom ocjena iz intervala 1-3 za svaku klasu prijetnji

Prosjekom pojedinačnih ocjena klasa prijetnji

Sumom ocjena iz intervala 1-20 za svaku klasu prijetnji

Sumom umnožaka vjerojatnosti i štete za svaku klasu prijetnji

Sumom ocjena iz intervala 1-5 za svaku klasu prijetnji

**42 Faze odgovora na incident su**

Detekcija, Analiza, Reakcija, Oporavak

Detekcija, Reakcija, Oporavak, Verifikacija

Planiranje, Detekcija, Reakcija, Oporavak <--

Planiranje, Detekcija, Inspekcija, Reakcija

Planiranje, Analiza, Provedba, Verifikacija

**43 Pri modeliranju slučajeva zloporabe koriste se stereotipovi**

Threaten, Mitigate

Attack, Defend

Request, Response

Exploit, Block

Try, Catch

**44 Automatski nastavak rada na pričuvnom poslužitelju, računalnoj ili mrežnoj komponenti naziva se**

Backover

Failback

Switchback

Switchover

Failover <--

**45 Fuzzing (pročešljavanje) je tehnika**

Provjere poslovnih procesa

Analize podataka

Dinamičke provjere <--

Određivanja ranjivosti

Statičke analize

**46 Plan koji se bavi prvom, neposrednom reakcijom na štetni događaj je**

Plan odgovora na incident <--

Plan kontinuiteta poslovanja

Plan upravljanja rizikom

Plan za nepredviđene situacije

Plan oporavka od katastrofe

**47 Fuzzing (pročešljavanje) je tehnika**

Dinamičkog testiranja <--

Analize sigurnosnih zahtjeva

Statičke analize

Inspekcije programskog koda

Penetracijskog testiranja

🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥🔥