Predmet:
BEZBEDNOST INFORMACIONIH SISTEMA

VISOKA POSLOVNA ŠKOLA STRUKOVNIH STUDIJA
NOVI SAD

OSNOVI ZAŠTITE INFORMACIJA

5. METRIKA SISTEMA ZAŠTITE INFORMACIJA

Cilj

- **Razumeti i naučiti:**
  - **terminologija** «*merenja*», »*metrike*» i «*metrički sistem*» ...
  - **značaj metrike** u oblasti zaštite:
    - ***proaktivni uticaj*** *na* ***digitalnu forenziku*** *i*
  - proces *razvoja metrika* i metričkog sistema
  - *metriku zrelosti procesa zaštite* na bazi SSE CMM
  - *tipične metrika* u oblasti zaštite IKT sistema

Definicije termina

- **Merenje***:*
  - **jednokratni uvid** u specifične merne parametre sistema zaštite
  - vrše se poređenjem u odnosu na predefinisani merni etalon
- **Metrika***:*
  - **višekratno merenje**, sredstvo za interpretaciju agregiranih mernih p.
  - **proizvod analize rezultata merenja** na višem nivou organizacije
  - objektivne ili subjektivne **interpretacije rezultata merenja**
  - od posebnog značaja za procese *digitalne forenzike*
- **Rezultati merenja***:*
  - objektivni i sirovi podaci koji se mogu automatski generisati
- **Metrički sistem:**
  - **skup** *kriterijuma, parametara, mernih uređaja, podataka i jedinica za generisanje i prikazivanje rezultata merenja*
  - podrazumeva procese *evaluacije* i *monitoringa* performansi SZ

Značaj metrike zaštite

- ***"Ničim ne može upravljati ako to ne može meriti"***
- **Ciljevi i kvalitet sistema zaštite**, mogu se postići na bazi:
  - *bezbednosnih zahteva za proizvode zaštite* (ISO/IEC 15408…)
  - *najbolje prakse zaštite* (NIST SP 800–53, ISO/IEC 27001/2…)
  - *procesnog pristupa i modela sazrevanja procesa* zaštite (SSE–CMM*)
- U **ISO/IEC 15443** – navedeni su svi metodi kvaliteta IKTS:
- **Vrednost metrike** - *konzistentna, ponovljiva i objektivna merenja*
- **Proaktivno obezbeđuje DF istragu**
- **Specifična metrika zaštiti** pomaže da se razume bezb. rizik

SSE–CMM*- *Security System Engeneering Capability Maturity Model,* standard **ISO/IEC 21827 od 2002.**

Metrika zaštite

- **Namena metrike zaštite** je da:
  - identifikuje **slabe performanse** mehanizama zaštite
  - **omogući** odgovarajuće **korektivne akcije**
- **Glavni principi metrike zaštite:**
  - ***imati informacije*** *koje se* ***mogu kvantifikovati*** *(%, srednje vrednosti, gradacije: nizak, srednji, visok)*
  - ***dostupnost podacima*** *koji podržavaju metrički sistem*
  - *samo* ***ponovljive procese*** *smatrati merljivim*
  - *rezultat upotrebljiv za praćenje performansi SZ i*
  - ***usmeravanje resursa*** *za zaštitu...*

Metrike zaštite

- **Najčešći metrički sistemi**:
  - *snaga kriptografskog algoritma*
  - *kvalitativna metrika* (npr. uticaja **R**: *nizak, srednji, visok*)
  - *kvantitativna metrika* (*cost-benefit* analiza tretmana rizika)
  - *metrika softverskog inženjerstva* (***SwE, SSE CMM***)
  - *detekcija anomalija* (**IDS/IPS**), *srednje vreme napada*
  - *intervjui , metrika poslovnih procesa, revizija sistema zaštite* i
- **Objekti merenja***:*
  - *organizacija, proizvod* (planiran, u razvoju, u radu), *tehnički sistem* itd.
- **Menadžment sistem zaštite informacija**:
  - *nema dobro definisane metrike*
  - *ne postoji konsenzus oko ključnih indikatora* (zbog skrivanja bezbednosnih incidenata)

Taksonomije metrike zaštite

- **U odnosu na generički tip**:
  1. **Kvantitativno/kvalitativna metrika** zaštite:
  - dostupna, izvodljiva za merenje i ponovljiva
  - pogodna za praćenje performansi i usmeravanje resursa
  2. **Rezultatski orjentisana metrika** (ciljeva zaštite):
  - meri performanse za **kontinualno poboljšanje** procesa z.
  - *metrika sazrevanja procesa zaštite* (**1 do 5 nivoa zrelosti**)*
  - evaluira efektivnost i poboljšava **U, O i T** procese zaštite
  - obezbeđuje relevantne podatke o izvršavanju ciljeva zaštite
- **U odnosu na objekte zaštite:**
  1. *kvaliteta implementacije politike zaštite*
  2. *efektivnosti i efikasnosti kontrola zaštite*
  3. *uticaja bezbednosno relevantnih događaja na poslovanje*
  4. *kombinacija sve tri metrike*

*__Razvijeno više modela -__ SSE–CMM postao *defacto* standard

Program metrike sistema zaštite

- **Zrelosti programa** utiče na **efektivnost svakog tipa**
  - zavisi od organizacije i kvaliteta implementacije k. zaštite
- Zahteva periodičnu analizu za **obuku, poboljšanje efektivnosti procesa i planiranje** kontrola zaštite
- Treba da **uključi najmanje** :

1. *Podršku menadžmenta*: kritična komponenta uspeha
2. *Politiku i procedure zaštite*: za nametanje i usaglašenost
3. *Uloge i odgovornosti za kvalitet zaštite:* na bazi rezultata metr.
4. *Metrike zaštite:* uputstva, metod, proces za razvoj faktore uticaja na implementaciju

Generički tok procesa metrike sistema zaštite

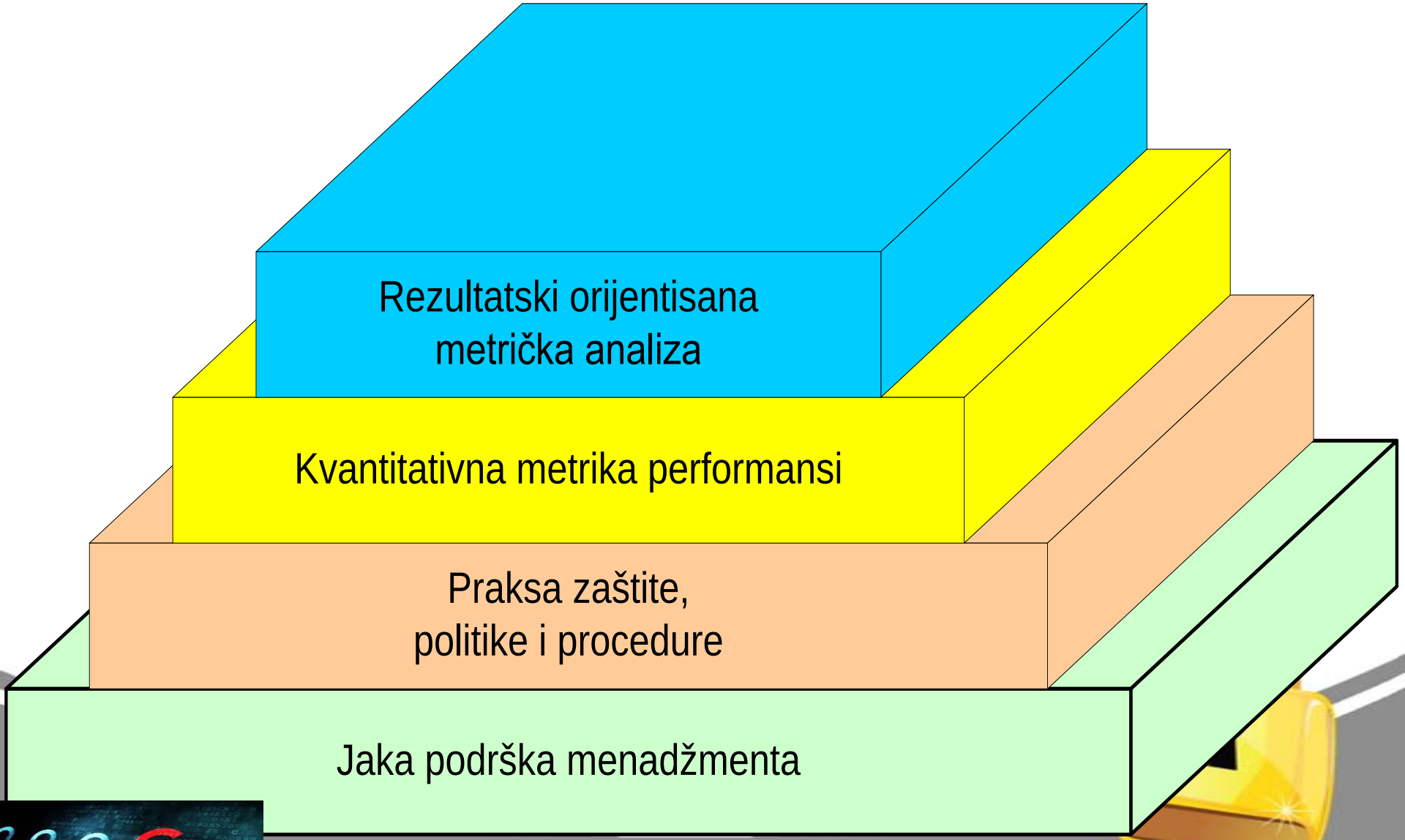
Definisanje bezbednosnih ciljeva i međuzavisnosti

Analiza i selekcija metričkih komponenti

Pronalaženje međuzavisnosti

Formiranje integrisane metrike

Struktura programa metrike zaštite



Proces implementacije *programa metrike zaštite*

- **Obuhvata sedam koraka**:

(1) definisanje strateških i taktičkih ciljeva programa metrike

(2) izbor metrika zaštite

(3) razvoj strategije za primenu metrika

(4) uspostavljanje referentnih performansi i ciljeva poboljšanja

(5) određivanje načina prezentovanja rezultata metrika

(6) definisanje akcionog plana i akcija i

(7) uspostavljanje formalnog ciklusa preispitivanja programa

Proces implementacije *programa metrike zaštite (1)*

Definisanje strateških i taktičkih ciljeva programa metrike

Izbor metrike

Razvoj strategije za primenu metrike

Uspostavljanje referentnih performansi i ciljeva poboljšanja

Određivanje načina prezentovanja metrike

Definisanje akcionog plana i akcija

Preispitivanje programa metrike

Izbor *metrike zaštite*

- **Obezbeđuje**:
  - **kontrolisan proces uspostavljanja programa** metrike z.
  - **konzistentnost sa ciljevima** i „**kako**, **ko** i **kada“**koristi rezultate
  - **prilagođavanje metrike z. okviru/modelu** za poboljšanje procesa **(**ako postoji**)**
- **Ako ne postoji –** koriste se pristupi:
  - *odozgo nadole* ili
  - *odozdo nagore*

Izbor *metrike zaštite 1*

1. **Pristup** *odozgo nadole* zahteva:
   - *definisanje ciljeva* programa zaštite
   - *identifikovanje specifičnih metrika* postizanja tih ciljeva
   - *merenje*
2. **Pristup** *odozdo nagore* zahteva da se:
   - *identifikovanje procesa, proizvoda, servisa zaštite* i dr., već izmerenih ili koje treba meriti
   - *razmatranje metrika,* koje se mogu izvesti iz tih merenja
   - *određivanje veze metrika sa ciljevima* programa zaštite

Primer: 1. Pristup *odozgo nadole*

- **Preduslov** - uspostavljeni ciljevi programa zaštite
- **Bolji za identifikovanje metrika usaglašene sa ciljevima programa zaštite**

PRISTUP ODOZGO NADOLE	
1. Navesti ciljeve programa zaštite	**Primer ciljeva**: do kraja sledeće godine redukovati broj virusnih infekcija za 30%
2. Identifikovanje metrike za praćenje progresa svih ciljeva programa zaštite	**Primer metrike**: broj antivirusnih alarma u odnosu na presek stanja od pre dve godine
3. Odabrati merenja potrebna za svaku metriku	**Primeri merenja**: – *broj antivirusnih alarma po mesecu* – *broj prijavljenih infekcija*

Primer 2: Pristup *odozdo nagore*

- **Preduslov** - uspostavljeni procesi/proizvodi programa zaštite
- **Lakši za određivanje metrike**

PRISTUP ODOZDO NAGORE	
1. Identifikovati merenja za dati proces zaštite	**Primer merenja**: *prosečan broj detektovanih ranjivosti prvog stepena na svakom serveru po odeljenjima*
2. Određivanje metrike koja bi se mogla izraditi na osnovu odabranih merenja	**Primer metrike**: *promena broja kritičnih ranjivosti detektovanih na serverima od poslednjeg izveštaja o ranjivostima*
3. Određivanje veze između izvedenih metrika i uspostavljenih ciljeva programa	**Cilj**: *redukovati nivo detektovanih ranjivosti na serverima*

Karakteristike metrika zaštite informacija

- Sve metrike zaštite informacija imaju definisane neke *osnovne karakteristike*
  - omogućavaju *konzistentnost primene, izbor, komparaciju i analizu*

Karakteristike	Komentar
Naziv	Razumljiv naslov ili naziv koji opisuje metriku
Namena	Čemu služi metrika?
Cena	Procena **stvarnih troškova prikupljanja podataka** za izradu metrike
Tip	Tehnička ili proceduralna, savremena ili zastarela, numerička ili tekstualna
Lokacija	• gde mogu da se prikupe podaci za metriku zaštite • gde se nalaze podaci korišćeni u prethodnim metrikama • gde su primenjene prethodne metrike zaštite
Frekvencija	Koliko često treba prikupljati podatke i prezentovati metriku zaštite

Primeri: Metrike zaštite

- **Najčešći primeri metrika zaštite** informacija :
  - *usklađenost sa zakonima i regulativama,*
  - *demonstracija značaja zaštite informacija za organizaciju,*
  - *određivanje efektivnosti kontrola zaštite,*
  - *broj incidenata u datom vremenskom periodu i*
  - *performanse zaštite u odnosu na budžet*
- **Metrike zaštite informacija** treba da:
  - daju kvantitativne, konzistentne i ponovljive rezultate
  - obezbede osnovu za:
    - *analizu efektivnosti programa zaštite i izveštavanje*
    - *razumevanje načina održavanja sistema zaštite informacija*
    - *demonstraciju vrednosti zaštite informacija za poslovanje*

Primeri: Metrike zaštite po kategorijama

Karakteristike	Komentar
Kategorija	• broj pojave određenih događaja (**broj**) • ponavljanje događaja (**frekvencija**) • vreme utrošeno na događaj (**trajanje**) • troškovi događaja (**cena**)
Start/stop kriterijumi	• prikupljanja podataka za metriku • upotrebe i prezentovanja metrike
Trajanje prikupljanja	Utvrđivanje vremenskog perioda potrebnog za prikupljanje podataka
Period upotrebe	Procena vremenskog perioda u kom će metrika biti korišćena

Primeri: Metrike zaštite po kategorijama

Kategorija	Primeri
Broj (koliko puta se nešto dogodilo)	• bezbednosnih događaja • blokiranih poslovnih *e–mails* • izvršenih bekapovanja • nove informacione imovine • propusta osoblja odgovornih za zaštitu • sprečavanja korišćenja osetljivih dokumenata • sprečavanja korišćenja zaštićenih aplikacija

Primeri: Metrike zaštite po kategorijama

Kategorija	Primeri
Frekvencija (koliko često se nešto događa)	• incidenata • revizije dokumenata • dodele privilegija • provere (*audit*) kontrole pristupa • pristupanja web lokacijama • bekapovanja servera • fizičkih pristupa server sali

Primeri: Metrike zaštite po kategorijama

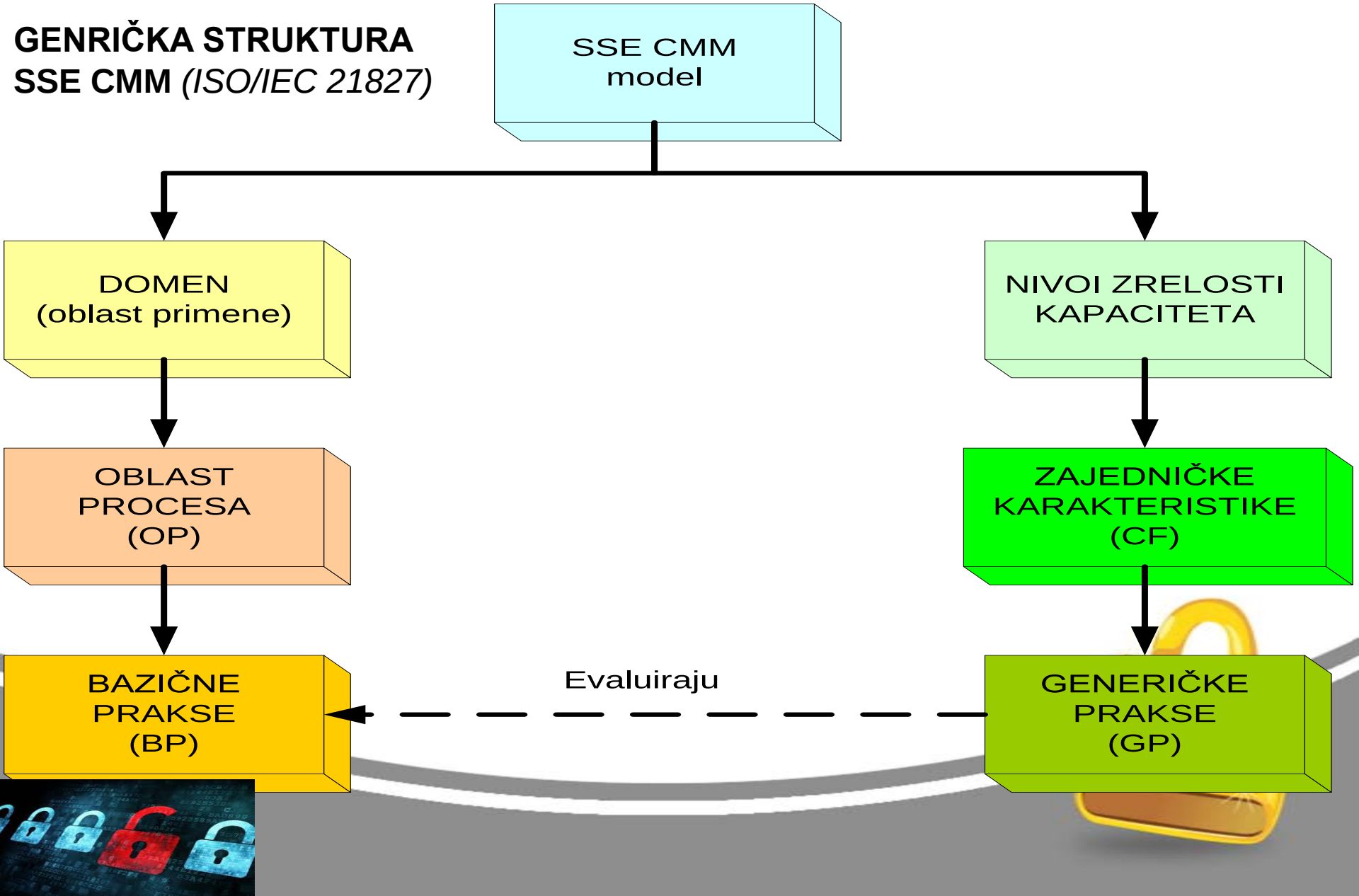
Kategorija	Primeri
Trajanje (koliko dugo je događaj trajao)	• incidenta • bekapovanja • izloženosti pretnjama • reagovanja na incidente • pečovanja (bezbednosnih popravki) • oporavljanja • monitoringa

Primeri: Metrike zaštite po kategorijama

Kategorija	Primeri
Cena (koliki su gubici zbog događaja)	• rešavanja događaja ili zamene oštećene imovine • saniranja incidenta • vraćanja u prethodno stanje (oporavak) • kontrola zaštite • administracije • sudskih procesa • edukacije

Procesno orijentisani metrički sistem

GENRIČKA STRUKTURA
SSE CMM *(ISO/IEC 21827)*



Atributi sazrevanja procesa SSE CMM

5. OPTIMALAN PROCES:
KUP, menja se i adaptira da postigne relevantne poslovne ciljeve

4. KVANTITATIVNO UPRAVLJAN PROCES (KUP):
DP statistički kvantitativno kontrolisan u toku projekta, obezbeđuje predviđanje performansi procesa

3. DEFINISAN PROCES (DP):
UP skrojen od standardnih **P**. org., detaljno opisan, rigorozno izvršavan, povećava vredn. proizvoda rada

2. UPRAVLJAN PROCES (UP):
IP, planiran sa politikom zaštite, monitorisan, kontrolisan, postiže planirane ciljeve performansi

1. IZVRŠEN PROCES (IP):
postiže produktivnost za proizvodnju proizvoda rada

Atributi sazrevanja procesa SSE CMM 1

- **Metrika SSE–CMM modela sazrevanja procesa zaštite**
  - **0. nivo** – bez aktivnosti i izvršenih procesa zaštite (obično se u modelu izostavlja)
  - **1. nivo** – nekompletan i neformalno izvršavan, postoji politika zaštite
  - **2. nivo** – kompletiran, dokumentovan, praćen, postoje detaljne procedure
  - **3. nivo** – dobro definisan, implementirane i dokumentovane procedure
  - **4. nivo** – kvantitativno meren, verifikovan, testirane usaglašenosti sa politikom
  - **5. nivo** – kontinualno poboljšavan, potpuno implementirane u celom IKTS

Procesno orijentisani metrički sistem

- **SSE CMM metrički sistem** obuhvata:

1. **Procesno orijentisanu metriku:**
   - definiše se sa kvantitativno/kvalitativnim dokazima o **nivoima zrelosti *oblasti procesa*** ili
   - **binarnom indikacijom** prisustva/odsustva zrelog procesa
2. **Rezultatski orijentisanu metriku** obezbeđuje**:**
   - dokaz **efektivnosti procesa**
   - **atribute rezultata merenja -** objektivne/subjektivne, kvalitativne/kvantitativne

Procesno orijentisani metrički sistem 1

- ***Metrika sazrevanja procesa* zahteva**:
  - prikupljanje i *verifikaciju* dokaza o izvršenim aktivnostima
  - korišćenje resursa organizacije
  - analizu aktivnosti sa snabdevačem
  - primenu metoda merenja
  - tačnost, ponovljivost i nezavisnost procesa itd.
  - **definisanje skupa mernih atributa** za:
    - *neprekidno poboljšavanje procesa zaštite*
    - *kvantitativno merenje i praćenje standardnih procesa org.*
    - *podršku, planiranje i upravljanje procesima organizacije*
    - *izvršavanje i izveštavanje procesa organizacije*

Procesno orijentisani metrički sistem 2

- **Izbor SSE CMM metrika** zavisi od **zrelosti programa zaštite** :
  - koji **implementira mehanizme za praćenje** i dokument.
  - vrši **kvantitativnu verifikaciju** performansi sistema zaštite
- **Više podataka - lakše merenje** i mogućnost automatizacije
- **Podaci iz automatizovanih alata mogu biti korisni**:
  - za *nadzor i sertifikaciju* sistema zaštite
  - *analizu baza podataka* i drugih izvora informacija
- **Sa aspekta zrelosti programa zaštite postoje**:
  - **tri tipa** metričkih sistema zaštite

Tipovi metrika zaštite

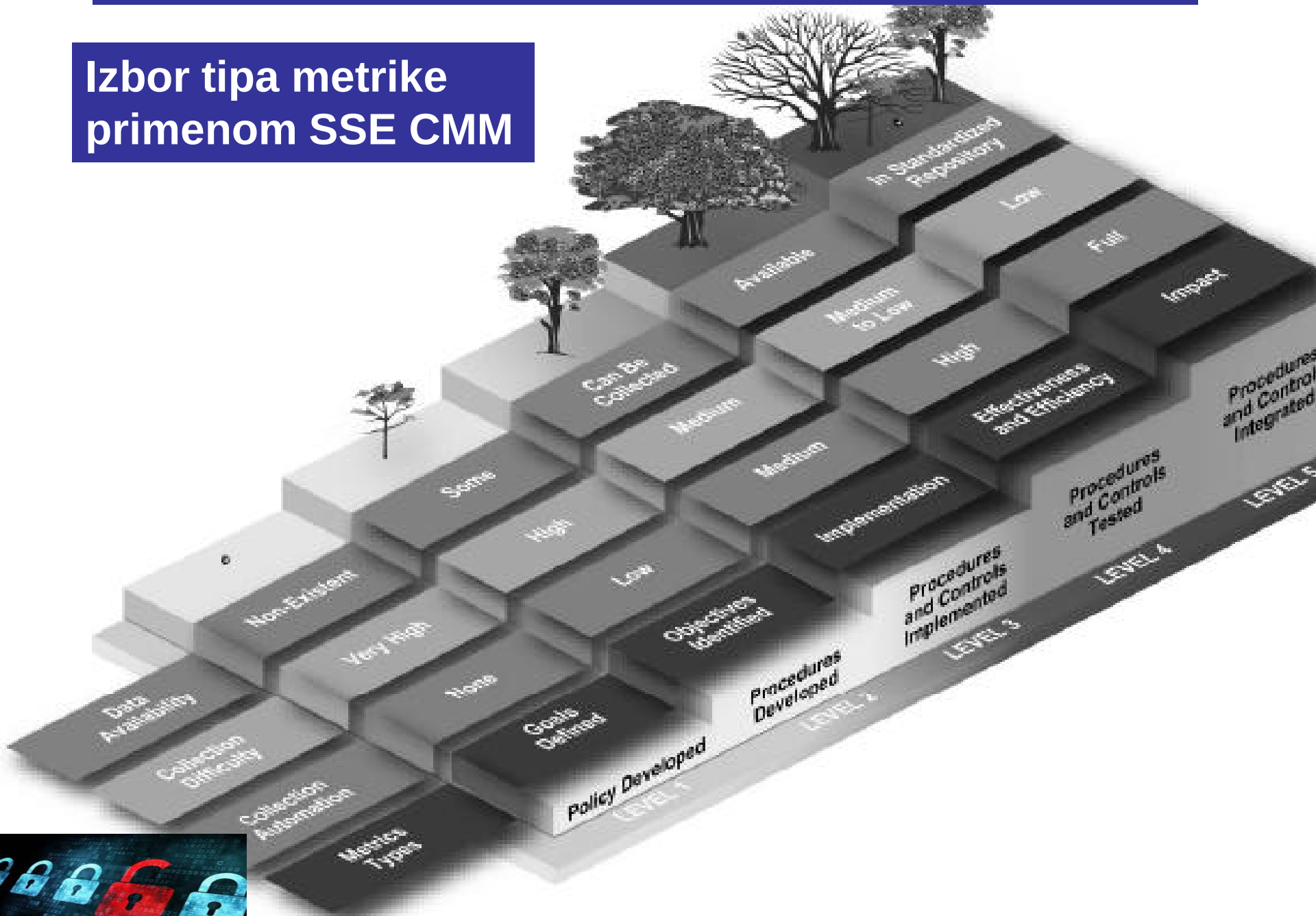
- **1. Tip** *(do 3. nivoa zrelosti):*
  - *procenat sistema* sa odobrenim planovima zaštite, politikom lozinke i AC
  - implementacija kontrole zaštite 100% izvršena – (S/Z na 3. nivu zrelosti)
- **2**. **Tip** (*4. i 5. nivo zrelosti*):
  - podaci o performansama programa zaštite su dostupniji
  - metrika fokusirana na *efikasnost* i *efektivnost* kontrola zaštite

    Primer: **%** lozinki za koje je vreme, potrebno za krekovanje, usaglašeno sa politikom zaštite lozinke.
- **3. Tip** (*5. nivo zrelosti*):
  - skupljanje mernih podataka potpuno automatizovano
  - meri **uticaj bezb. događaja na poslove organizacije**

    Primer: merenje uticaja obuke sa **%** obučenih korisnika i administratora

Primer: Izbor tipa pocesno orijentisane metrike

Izbor tipa metrike primenom SSE CMM



Razlozi za primenu metrika zaštite

- **Osnovni razlozi za primenu metrika zaštite**:
  - *veći kvalitet menadžment sistema zaštite*
  - *usaglašavanje sa zakonima i standardima*
  - *efikasnost i efektivnost performansi procesa zaštite u odnosu na ciljeve zaštite*
  - *demonstracija značaja zaštite za organizaciju*
  - *podrška proceni rizika*
  - *proaktivna digitalna forenzika itd.*

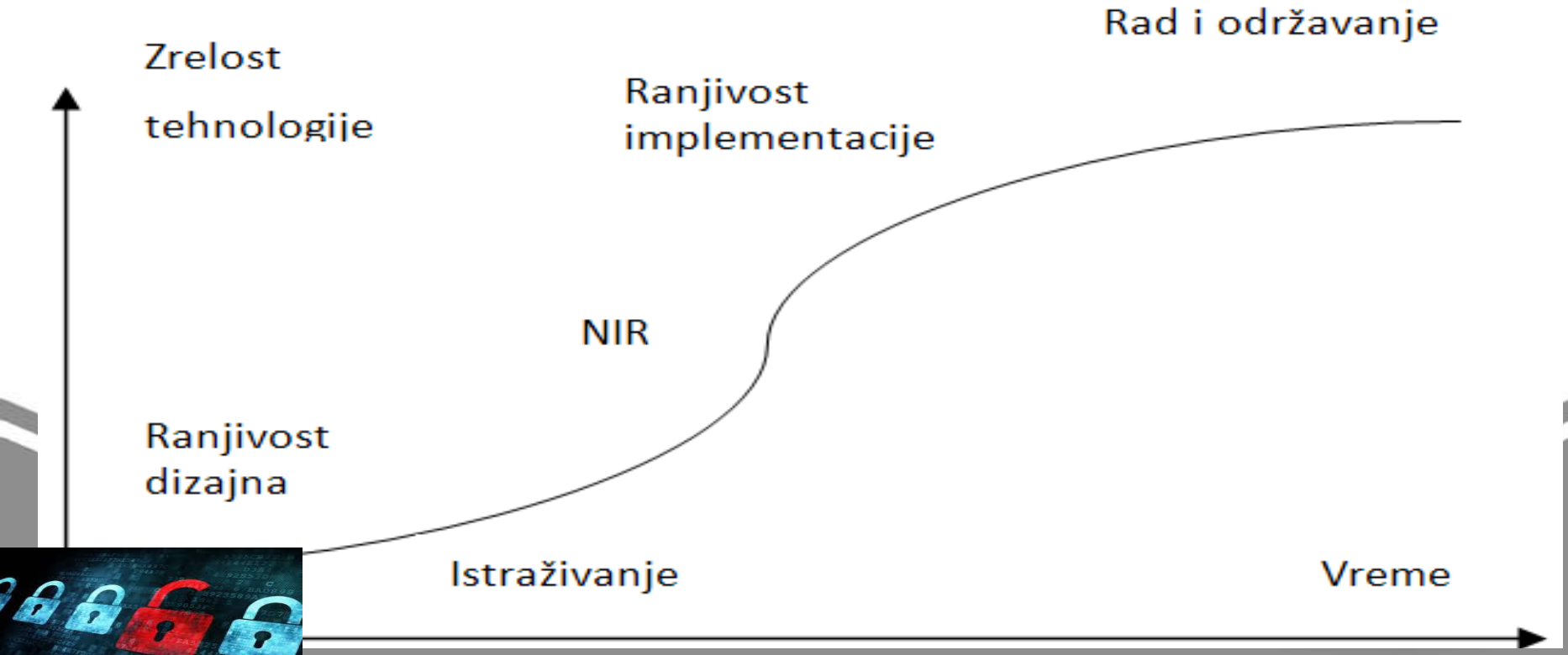
Tehnički metrički sistemi

- **Tehnički metrički sistemi** mogu se primeniti za:
  - *uspostavljanje cilja zaštite* – merenje stepena dostizanja cilja
  - *planiranje nivoa zaštite* – predviđanje pre implementacije
  - *implementirani sistem* – za merenje nivoa upada (IDPS)
  - *usaglašavanje* – merenja usklađenosti sa std.i politikom
  - *nadzor* – skeniranje nivoa zaštite nekog objekta
  - *analizu* – kao metod za izbacivanje grešaka

Primeri tehničkih alata za merenje nivoa zaštite:
- *IDPS, skeneri mrežne zaštite, antispam i AVP, firewalls*
- generišu merne podatke i smeštaju u log datoteke zaštite
- trend je merenje zaštite iza IDPS (prema Internetu)

Primer: Metrika proizvoda zaštite

- može se primeniti u svim tačkama ranjivosti i fazama životnog ciklusa (razvoja, implementacije i održavanja) proizvoda zaštite
- zavisno od zrelosti primenjene tehnologije metrika evoluira i stabiliše se u fazi održavanja



Primer: Intervju kao metrički sistem

- **Indikator**: *inicijalne slike* stvarnog stanja
- **Broj uzoraka**: dovoljan za uopštavanje rezultata
- **Oblasti za prikupljanje informacija**:
  - *kritični elementi* sistema zaštite (npr. pristupne tačke Internetu)
  - *U, O i T kontrole*, *organizacija, okruženje i ciljevi zaštite*
  - *metrički sistemi (*npr. primenjeni standardi i dokumentacija*) i njihova implementacija*
  - *menadžment rizika i sistema zaštite itd.*
- **Kontrolni upitnici**:
  - ***7-8** tema i **20** pitanja* o zaštiti informacija
  - intervjuisanje, skupljanje, analiza i interpretiranje rezultata

Primer: Najčešće korišćene metrike zaštite

Metrika zaštite	Primer prikupljanih podataka
Incidenti	broj incidenata u određenom periodu...
Zaštita od virusa	broj incidenata određenog tipa virusa...
Upravljanje rizikom	broj izvršenih analiza rizika...
Upravljanje pečevima	broj popravljenih ranjivosti (u nekom periodu)...
Usaglašenost sa politikom zaštite	broj povreda politike zaštite...
Nalazi revizije	broj neusaglašenosti otkrivenih revizijom ...
Troškovi	ukupni gubici zbog bezbednosnih incidenata

Metrika operativnih kontrola zaštite

- **Treba da bude *SMART*:**
  - ***S**pecifična* – usmerena na oblast merenja, a ne sporedni proizvod ili rezultat
  - ***M**erljiva* – podaci moraju biti laki za skupljanje, tačni i kompletni
  - ***A**kciona* – razumljivi merni podaci za koje je lako preduzeti akciju
  - ***R**elevantna* – merenje samo onih podataka koji su važni za metriku
  - ***T**imely* (***Blagovremena***) – podaci moraju biti dostupni kada su potrebni

Primeri: Operativne metrike kontrola zaštite

Operativna metrika kontrola zaštite	Primer
Metrika AVP	*broj sistema sa aktivnim AVP*
Metrika upravljanja korisničkim nalozima	*broj naloga koji nikad nije korišćen*
Metrika logičke barijere (*firewall*)	*broj detektovanih obrazaca napada*
Metrike spama i integriteta sadržaja *e–pošte*	*broj procesiranih poruka e–pošte*
Metrika pristupa Internetu	*pokušaji pristupa zabranjenim web lokacijama*
Metrika nadzora politike zaštite	*procenat sistema popravljenih na zahtev korisnika*

Program metrike AVP zaštite

- Ključni elementi politike zaštite svake organizacije
- Merenje AVP je kritično za sprečavanje većeg uticaja na poslove
- Centralizovano upravljanje sistemom AVP zaštite
- Logovanje i izveštavanje za kreiranje korisne metrike

Primeri metrika za skupljanje podataka za sedmičnu analizu:

– *broj sistema sa aktivnim AVP*

– *ukupan broj sistema na koje treba instalirati AVP*

– *broj sistema bez ažuriranih AVP definicija*

– *broj sistema koji nisu nedavno skenirani na viruse (najmanje jedan put sedmično) i dr.*

Metrike upravljanja korisničkih naloga

- Značajna **zbog velikog broja internih napada**
- Monitoring i kontrola korisničkih naloga pomaže da se spreči njihovo korišćenje za napade na IKTS

Primeri metrika koja se mogu sakupiti i analizirati:

- *ukupan broj naloga, broj naloga koji nikad nije korišćen*
- *broj naloga koji nije korišćen 30 ili 60 dana*
- *broj administratorskih naloga i broj naloga servisa*

Metrike logičke barijere *(firewals)*

- Brojne su i mogu se monitorisati i kontrolisati
- Događaji na barijeri mogu ukazati na indikatore napada ili zloupotrebe internih konekcija IKTS

Primeri metrika koje se mogu sakupiti i analizirati:

- *broj ovlašćenih i dezaktiviranih konekcija (po tipu)*
- *količina informacija (u MB) procesiranih po tipu konekcije*
- *broj detektovanih obrazaca napada*

Metrike spama i integriteta sadržaja *e–mail*-a

- Važne su **u e-poslovanju**, zbog porasta spama
- Kontrole zaštite održavaju spam na određenom nivou i dopušta legitiman rad e–pošte

Primeri metrika koje se mogu sakupiti i analizirati:

- *broj procesiranih poruka e–pošte*
- *broj odbijenih poruka e–pošte zbog spama/restrikcije sadržaja*
- *količina odbijenih poruka e–pošte u MB (propusni opseg)*
- *broj odbačenih poruka e–pošte sa neodgovarajućim sadržajem i stopa lažnih identifikacija spama*

Metrika pristupa Internetu

- Značajno smanjuje destrukciju rada zaposlenih
- Smanjuje zakonske sankcije, zbog nepropisnog korišćenja Interneta
- Smanjuje troškove Internet opsega i gubitke produktivnosti zaposlenih

Primeri metrika koje se mogu sakupiti i analizirati:

- *glavni akteri zloupotrebe Interneta (vreme/MB korišćenja Interneta)*
- *pokušaji pristupa zabranjenim web lokacijama*
- *korisnička statistika vremena pretraživanja Interneta*

statistika pretraživanja Interneta iz poseta web lokaciji

broj datoteka preuzetih/blokiranih /zabranjenih

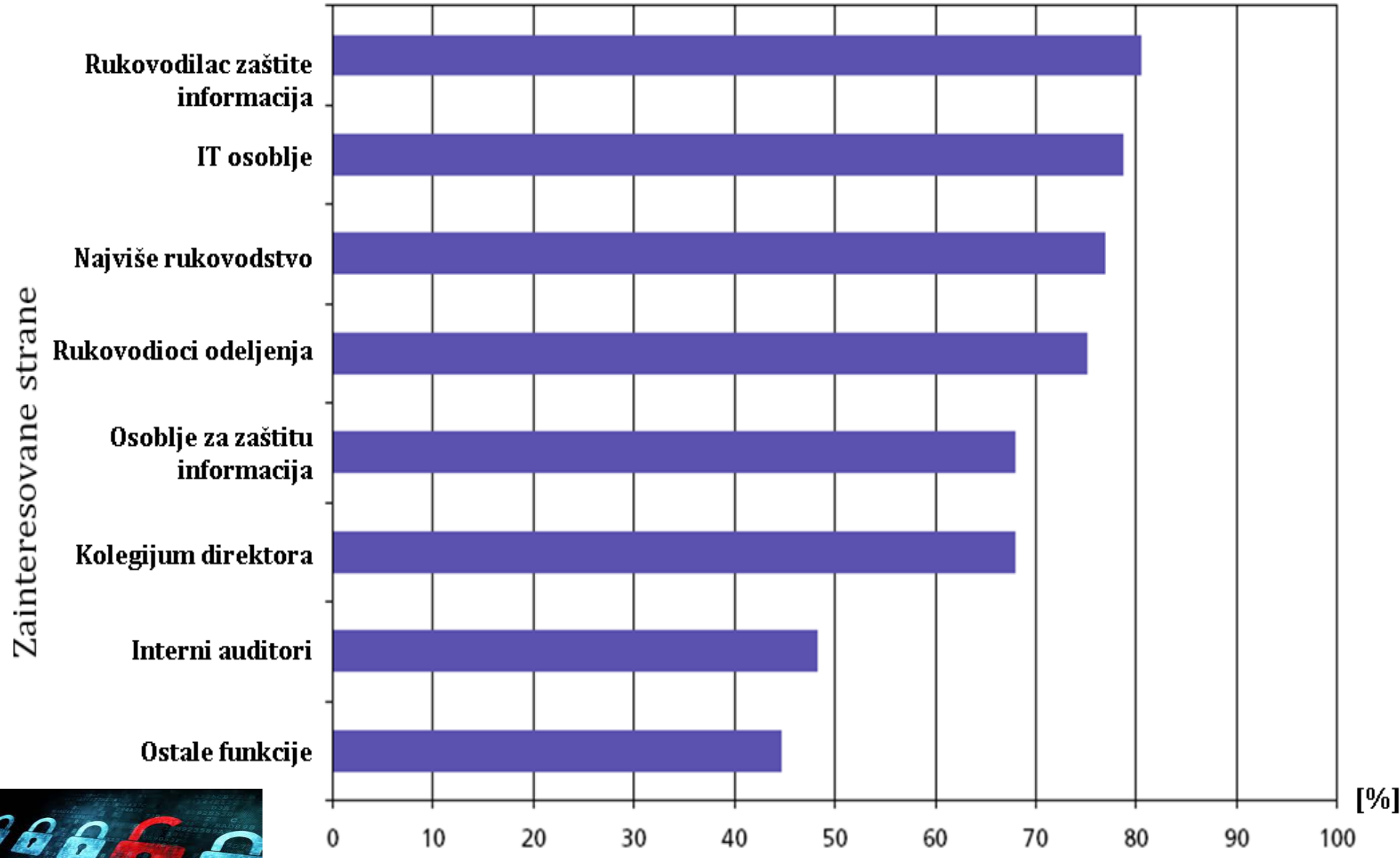
Metrika nadzora politike zaštite

- Značajna za *usaglašavanje* svih sistema sa standardima
- Aktivan monitoring program može identifikovati neusaglašenost
- Metrika može pokazati koliko je efektivna organizacija u sprečavanju/otklanjanju neusaglašenih sistema

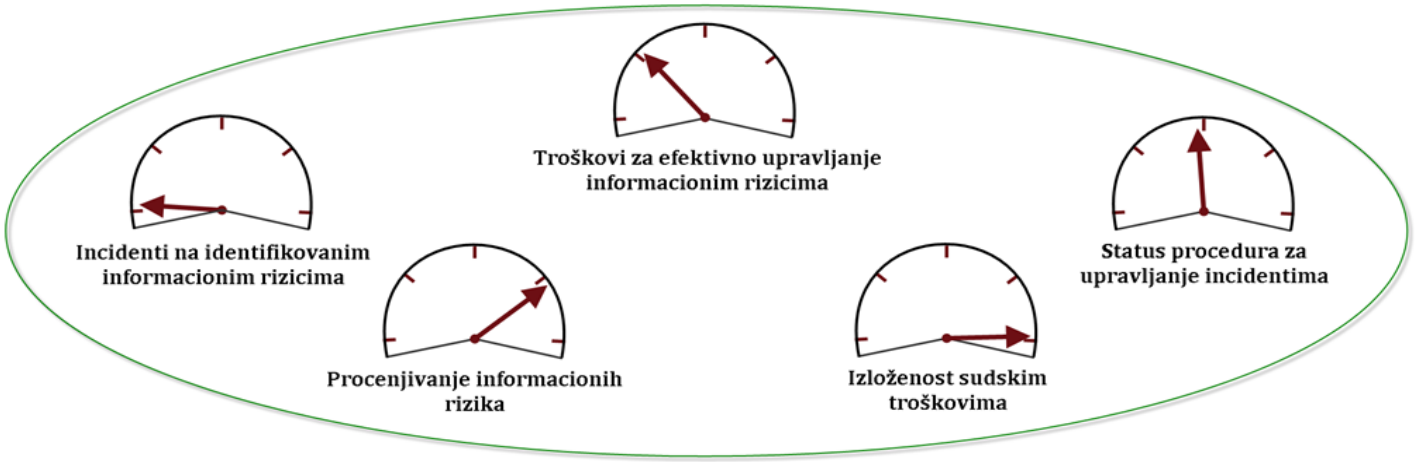
Primeri metrika koje se mogu sakupiti i analizirati:

- *procenat sistema usaglašenih sa standardima za zaštitu OS*
- *lista neusaglašenih sistema i pitanja koja se moraju obuhvatiti*
- *verifikacija statusa popravki*
- *procenat sistema popravljenih na zahtev*

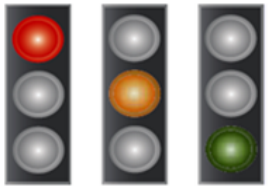
Primer: Pezentovanje metrika zaštite informacija



Primer: Forme prezentovanja rezultata metrika zaštite



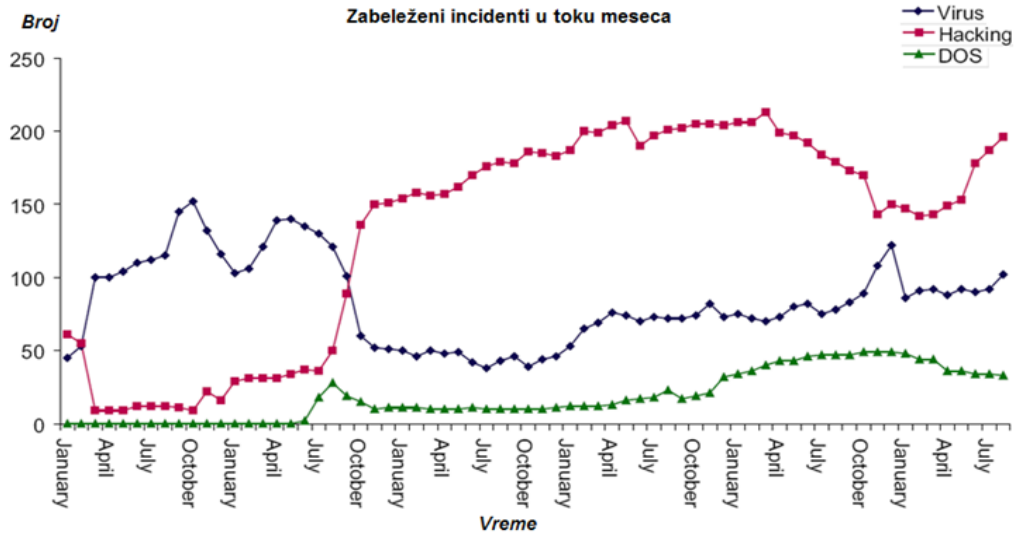
Instrument tabla



Semafori

Finansijski aspekt • Ciljevi: o Opstanak o Uspeh/rast o Prosperitet • Merenja: o Vraćene investicije o Protok novca o Rast prihoda o Curenje kapitala o Smanjenje cena	**Korisnički aspekt** • Ciljevi: o Akvizicija/zadržavanje/zadovoljenje korisnika o Profitabilnost • Merenja: o Zastupljenost na tržištu o Cene transakcija o Lojalnost/indeks/učešće klijenata o Odnosi sa dobavljačima o Najveći računi
Učenje i sazrevanja • Cinjevi: o Neprekidno unapređenje o Razvoj novih proizvoda • Merenja: o Produktivnost preduzetništva o Nove ideje/sugestije zaposlenih o Zadovoljstvo zaposlenih o Nivoi veština o Položaj osoblja o Zadržavanje zaposlenih o Profitabilnost po zaposlenom	**Interni poslovni procesi** • Ciljevi: o Ključne kompetencije o Kritične tehnologije o Poslovni procesi o Osnovne veštine • Merenja: o Efikasnost o Vreme iteracija o Pojedinačni troškovi o Godišnja stopa defekata o Vreme do tržišta

Komparativna tabela rezultata



Trendovi

Prednosti metrike zaštite

- *poboljšanje odgovornosti*
- *merenje svakog aspekta sistema zaštite*
- *izolovanje problema u zaštiti*
- *usaglašavanje sa zakonima*
- *angažovanje na proaktivnoj zaštiti*
- *merenje efektivnosti implementiranih kontrola zaštite* itd.

Nedostaci metrike zaštite

- **Problem**: *merenje uticaja ljudskog faktora* na metrike zaštite (**subjektivnost i** dr.)
- **Slabe** ili **neadekvatne implementacije**
- **Nedostatak ili nepostojanje**:
  - *jasno definisanih procesa metrike*
  - *svesti o potrebi upravljanja zaštitom*
  - *spremnosti menadžmenta za angažovanje u SZ*
  - *dokumenata zaštite, odgovornosti* itd.

Kriterijumi kvaliteta metrike zaštite

- Stepen uključivanja specifičnosti organizacije
- Upravljivost procesa i podataka
- Stepen zaštite baze mernih podataka
- Definisanost skupljanja mernih podataka
- Standardizacija izveštavanja o rezultatima merenja
- *Ponovljivost testiranja/merenja* digitalnih podataka
- Merenje forenzički relevantnih događaja
- Konvergencija sa proaktivnom forenzikom

Rezultati istraživanja primene metrika zaštite

1. Generalna definicija metrike zaštite
2. Najčešća primena na usklađenost sa zakonima
3. Najčešće za incidente, AVP, rizike, usklađenost i troškove
4. Obično se prezentuju menadžmentu i IKT osoblju
5. Mali broj se odnosi na netehnička pitanja
6. Retko se koriste za upravljanje poslovanjem
7. Često je teško odrediti kome i kako prezentovati
8. Definisanje ključnih koraka programa metrike
9. Primena kvantitativne i kvalitativne metriku
10. Da prezentacija odgovara potrebama korisnika

Primer: model istraživanja primene metrika zaštite

Komponenta	Primeri iz prakse	Primer problema u praksi
Cilj	upravljanje zaštitom informacija	teško praćenje poslovanja
Ulazni podaci	incidenti, AV zaštita	teškoće u izboru metrike
Prezentacija	razni načini prezentovanja raznim korisnicima	težak izbor prezentovanja neprecizan opis stanja zaštite

Pitanja