GDPR radionica, Klasificiranje podataka

- Nije blago ni srebro ni zlato, blago su informacije -

Agenda

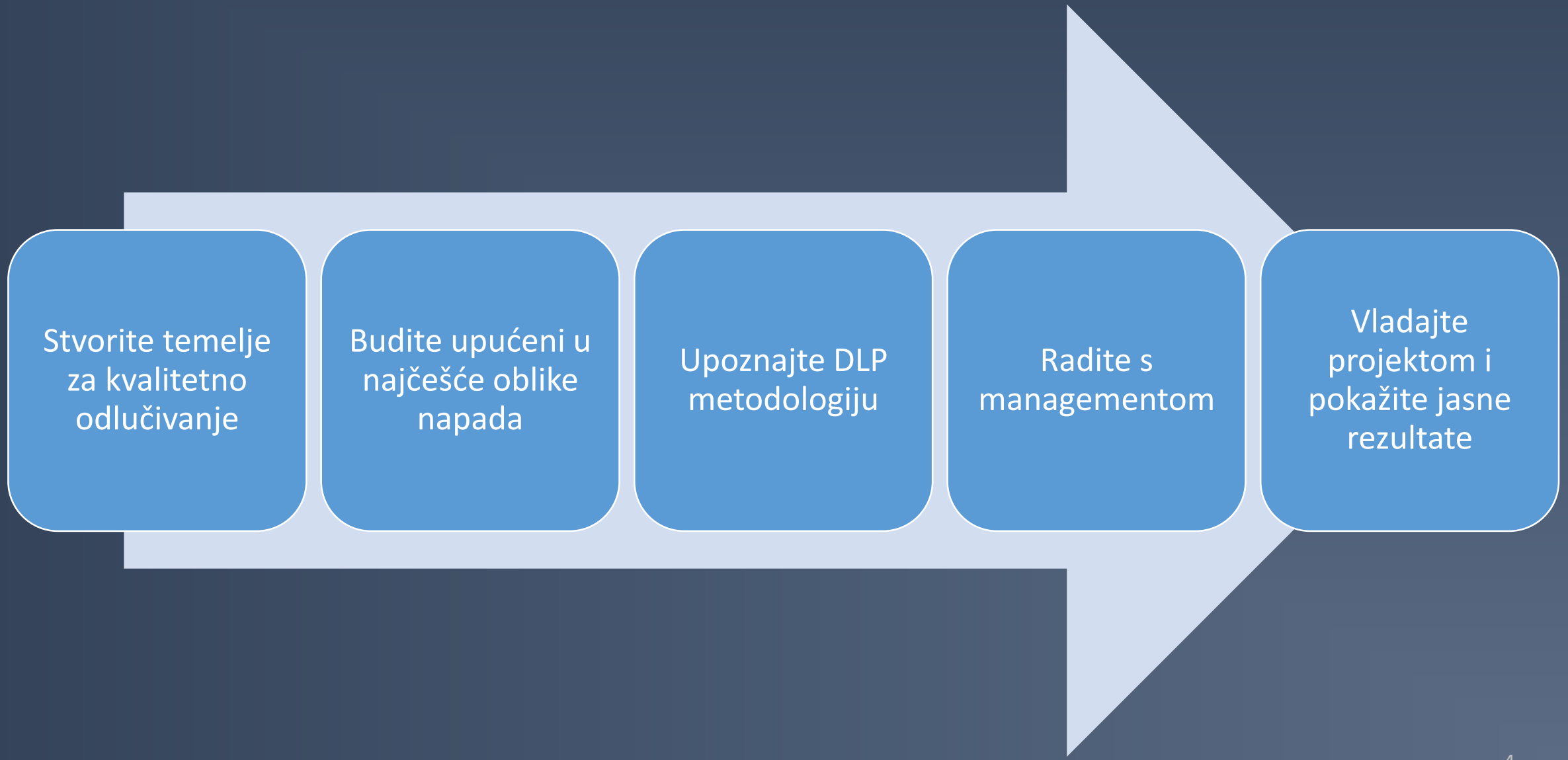
- Što je informacija i zašto se štiti?
- Kako stvoriti kvalitetno partnerstvo za projekt?
- Sigurnost: utvrđivanje rizika i postavljanje prioriteta.
- Dva osnovna načina pristupa projektu.
- Kako klasificirati informacije?
- Što je Data Loss Prevention i od čega se sastoji?
- Kako procijeniti DLP rješenja?
- Metoda implementacije kroz 9 koraka.
- Prikaz najvažnijih vendora i rješenja.
- Pitanja i odgovori

Što je informacija?

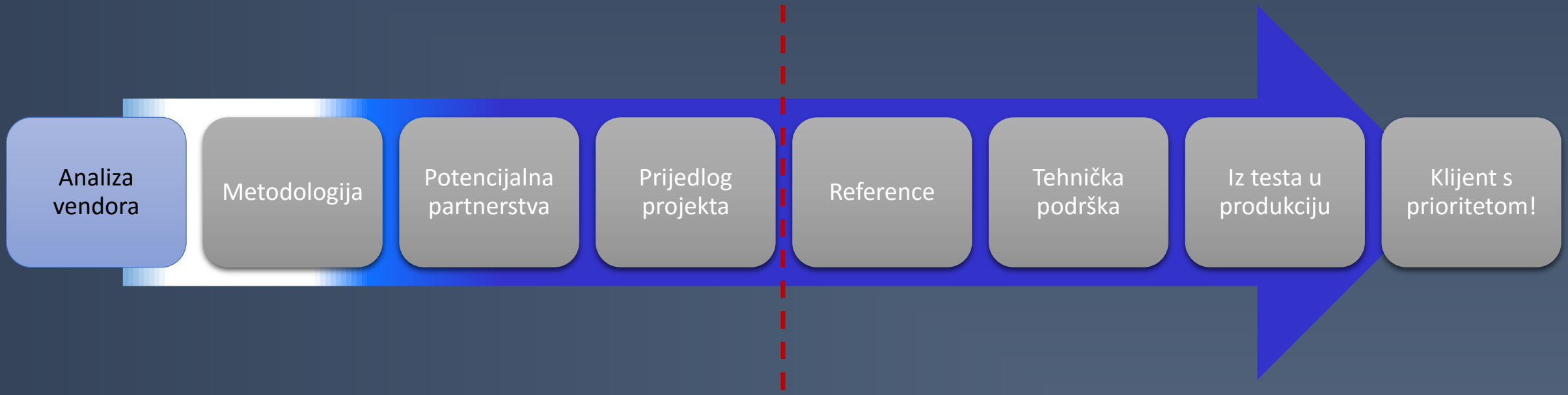
Jednostavno rečeno, informacija je primljena i shvaćena poruka. Ali prije svega, ona je rezultat procesiranja, manipuliranja i organiziranja podataka na način da isti nadograđuju znanje osobe koja informaciju prima.

Izvor: https://hr.wikipedia.org/wiki/Informacija

Strategija


Stvorite temelje za kvalitetno odlučivanje
Budite upućeni u najčešće oblike napada
Upoznajte DLP metodologiju
Radite s managementom
Vladajte projektom i pokažite jasne rezultate

Kako stvoriti kvalitetno partnerstvo

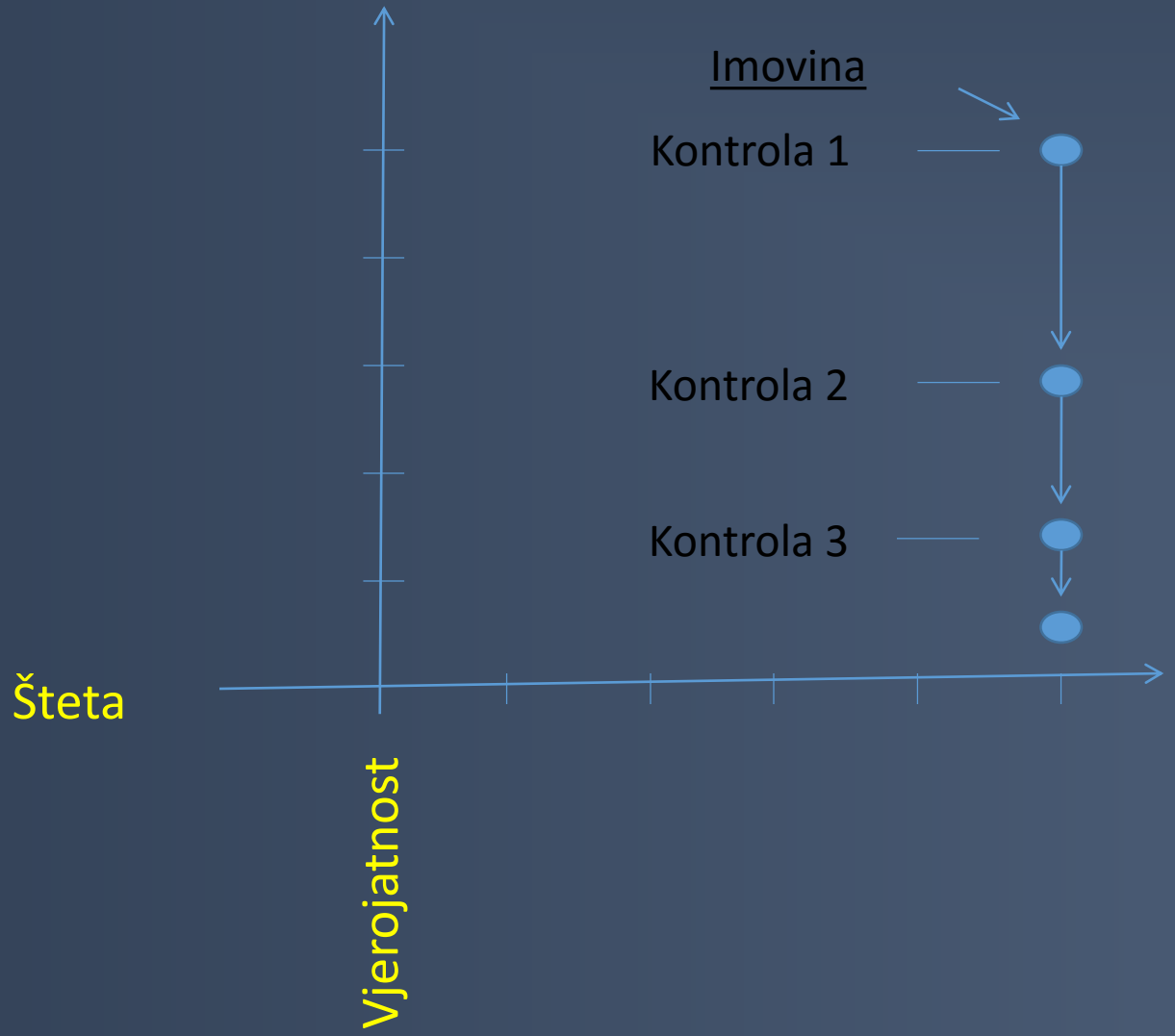


Sigurnosni aspekt i rizici

- Kako „radi” security?
- Što predstavlja rizike?

Sigurnost i rizici u sprezi

Rizik = (Šteta x % Vjerojatnost)



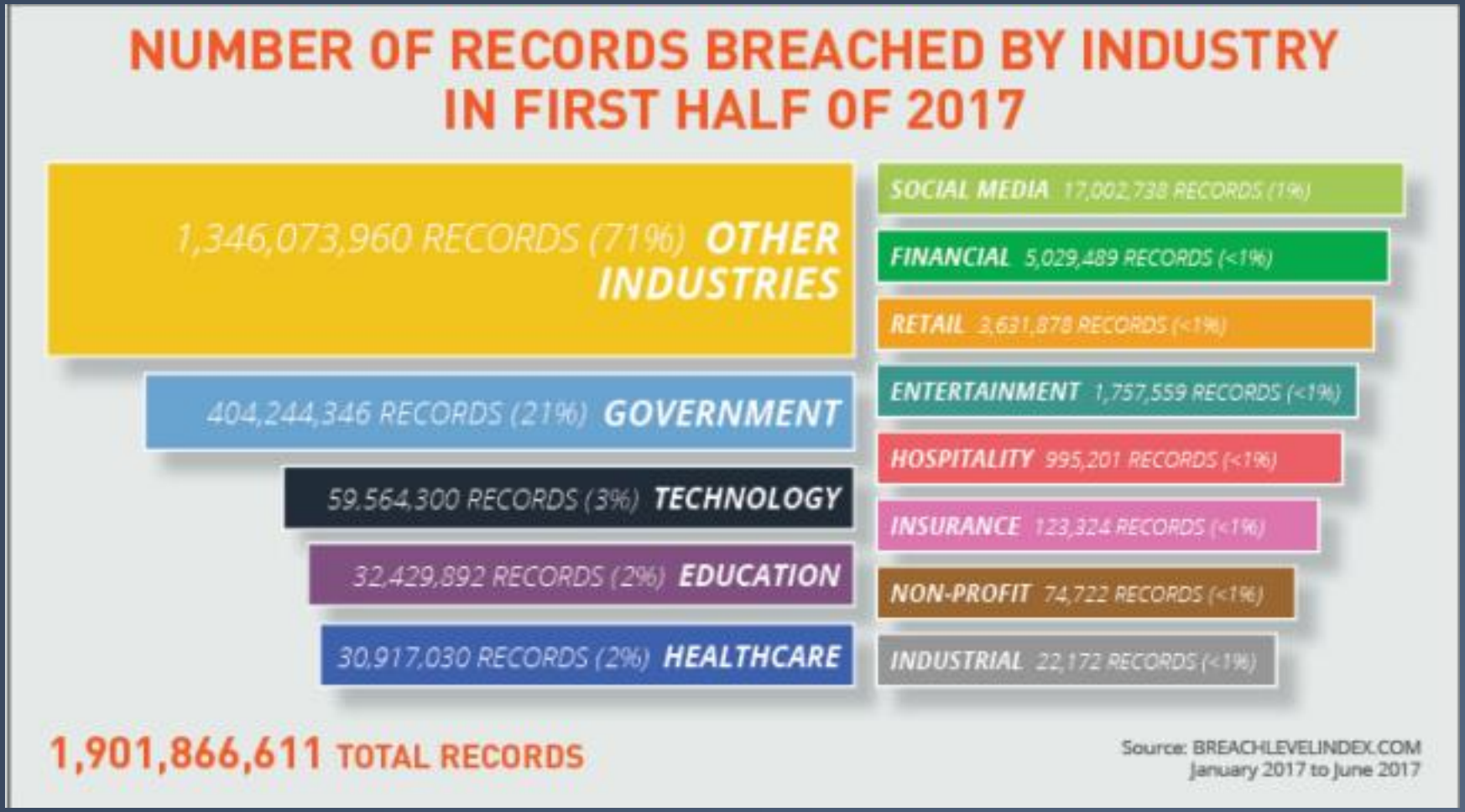
Osnovne vodilje

- Popis imovine (Assets)
- Kakva je moguća šteta?
- Koje su relativne prijetnje?
- Na štetu je teško utjecati.
- Možemo utjecati na vjerojatnost!

Osnovna pitanja

- Što ste do sada napravili da razumijete gdje se vaši podaci nalaze?
- Koja bi informacija (ili set informacija) u slučaju da je otuđena i završi u krivim rukama, mogla ozbiljno naštetiti vašem poslovanju?
- Što smatrate prijetnjama poslovanju?
- Vjerujete li da sigurnosni mehanizmi i procedure koje je vaša tvrtka implementirala, pružaju dovoljnu razinu zaštite?

Trendovi 2017



Izvor: https://blog.gemalto.com/security/2017/09/21/new-breach-level-index-findings-for-first-half-of-2017/

Kratki rezime

- Security JE disciplina – NIJE produkt ili rješenje
- Rizik = Šteta x % Vjerojatnost
- Ne možete mijenjati štetu – fokus je na vjerojatnosti
- Gubici podataka se svakodnevno događaju
- Četiri osnovna pitanja

Što je DLP?

Data Loss Prevention softver je rješenje koje sprječava otuđivanje i neovlašteno kopiranje podataka, koristeći: nadgledanje, otkrivanje i blokiranje prijenosa povjerljivih podataka.

Što je DLP?

DLP Kontrole

Identificiranje informacija

- U pokretu
- U korištenju
- Pohranjene

Metode identifikacije

- Opisane
- Registrirane (Finger-prints)

Što je važno?

DLP Vendori

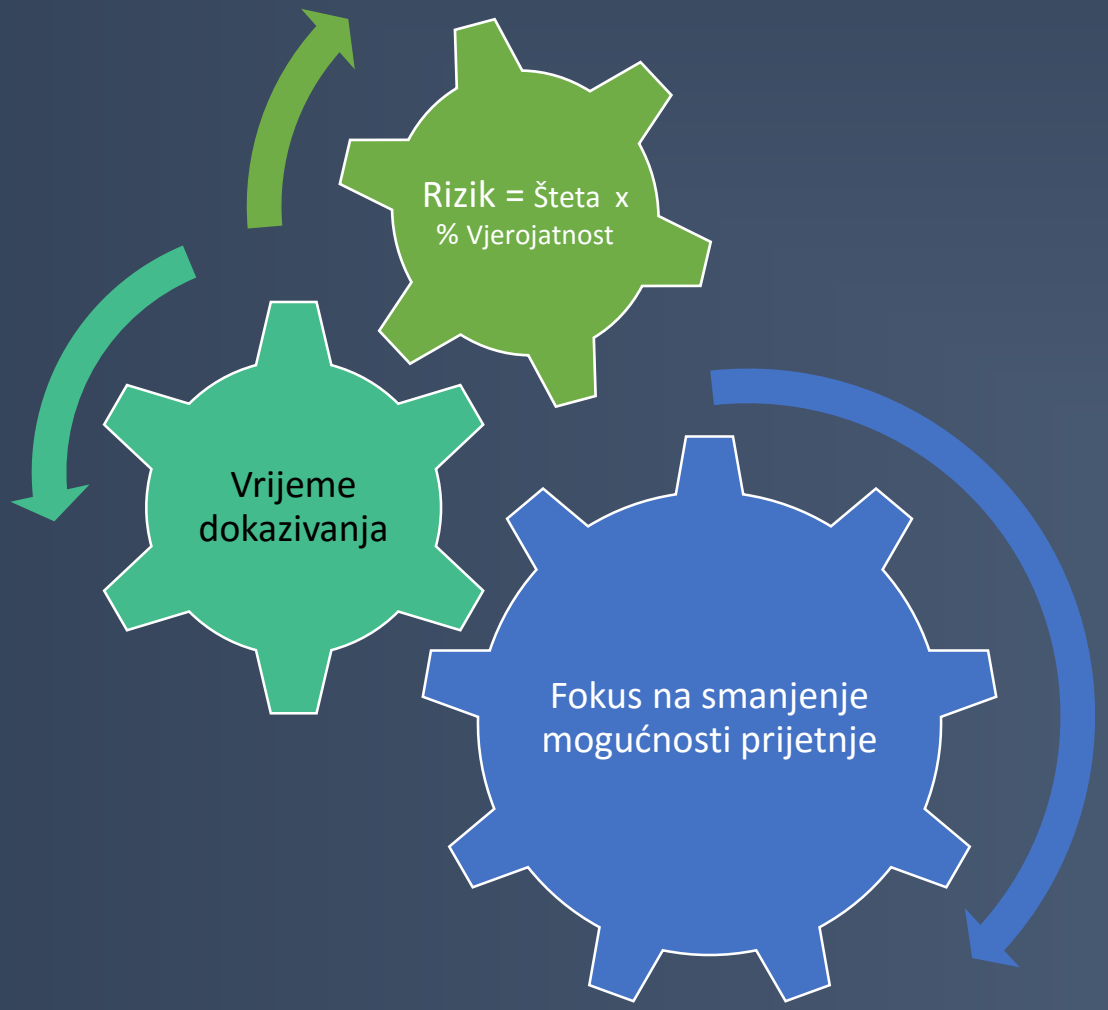
Metodologija

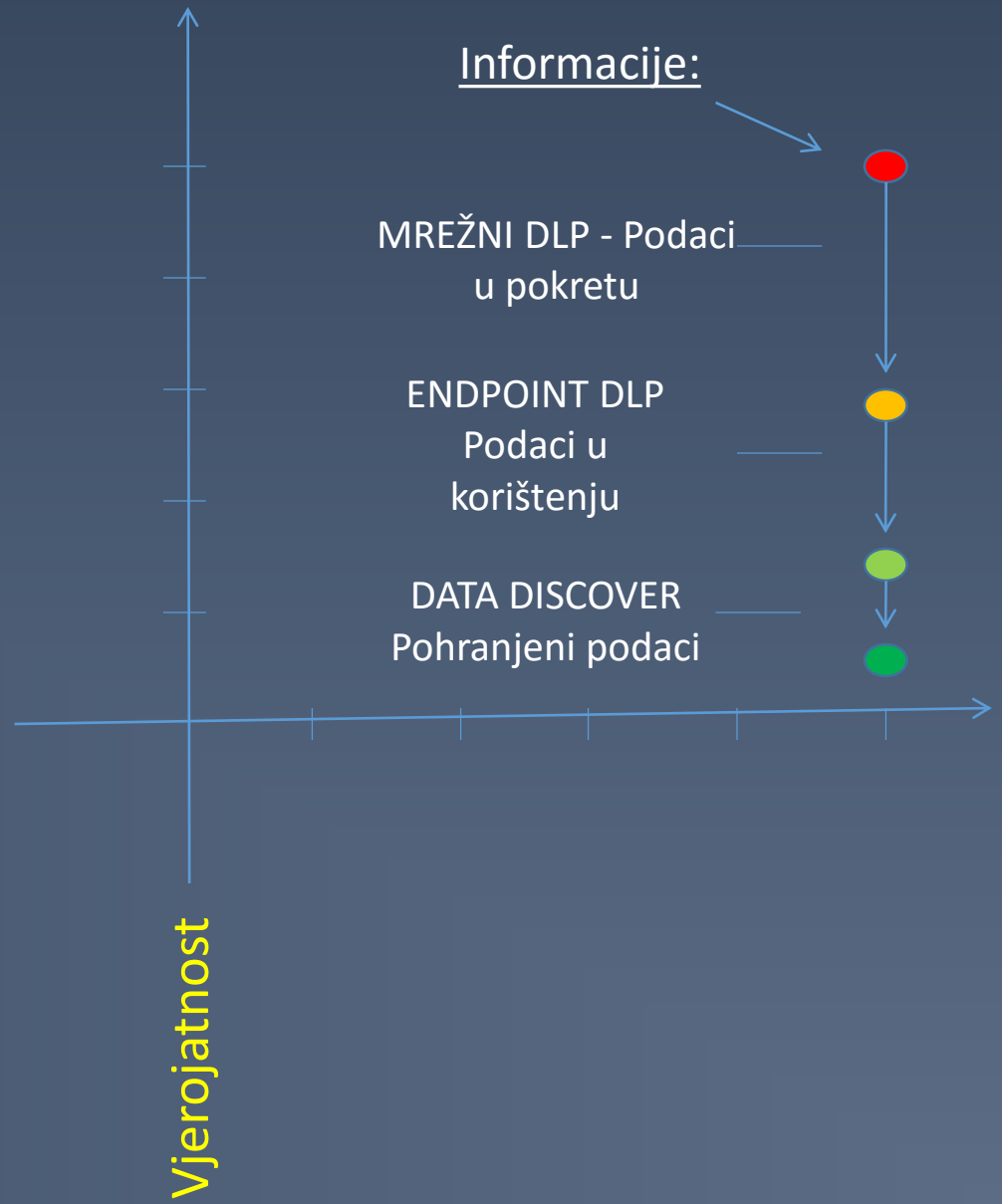
- Vizija
- Mogućnosti
- Planiranje

Projekt

- Pristup
- Cijena (TCO)
- Vrijeme dokazivanja

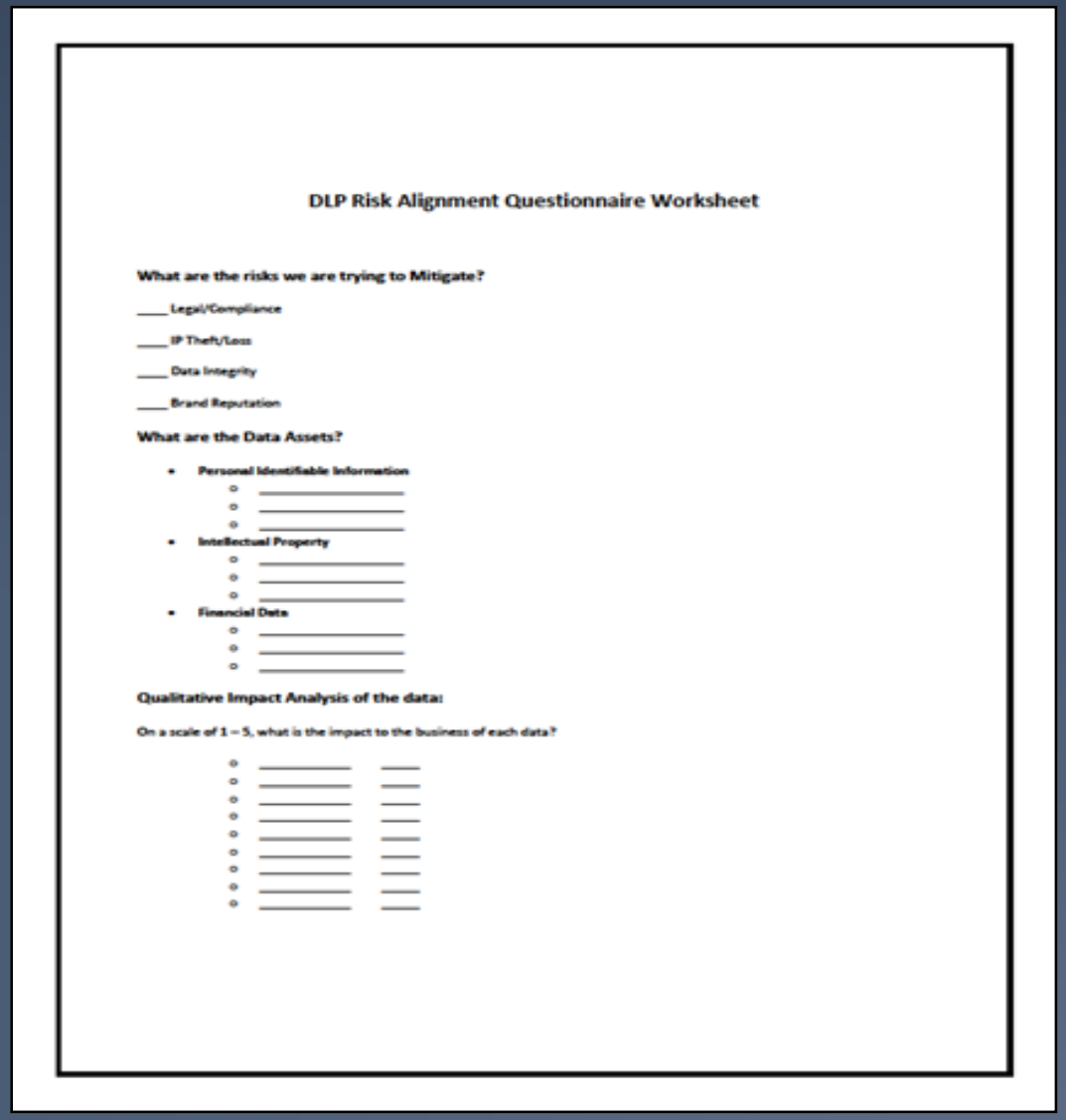
Strategija zaštite informacija





Korak 1: Napravite Information Risk Profile

1. Definirajte rizik koji želite adresirati.
2. Napravite listu nositelja podataka i grupirajte ih po tipu.
3. Intervjuirajte „vlasnike” podataka da bi razumjeli važnost i vrijednost istih.
4. Evidentirajte sve kanale putem koji se podaci mogu poslati.



DLP Risk Alignment Questionnaire Worksheet

What are the risks we are trying to Mitigate?

____ Legal/Compliance

____ IP Theft/Loss

____ Data Integrity

____ Brand Reputation

What are the Data Assets?

- **Personal Identifiable Information**
  - _____
  - _____
  - _____
- **IntelEectual Property**
  - _____
  - _____
  - _____
- **Financial Data**
  - _____
  - _____
  - _____

Qualitative Impact Analysis of the data:

On a scale of 1 – 5, what is the impact to the business of each data?

- _____ ____
- _____ ____
- _____ ____
- _____ ____
- _____ ____
- _____ ____
- _____ ____
- _____ ____
- _____ ____

Korak 2: Napravite pregled ključnih resursa

1. • Jasno definirajte tipove podataka koje želite zaštititi.
2. • Provjerite postojanost zakonskih i poslovnih regulativa s podacima (1).
3. • Odredite mehanizme za definiranje i klasificiranje podataka.
4. • Odredite ozbiljnost štete i način odgovaranja na potencijalni incident.

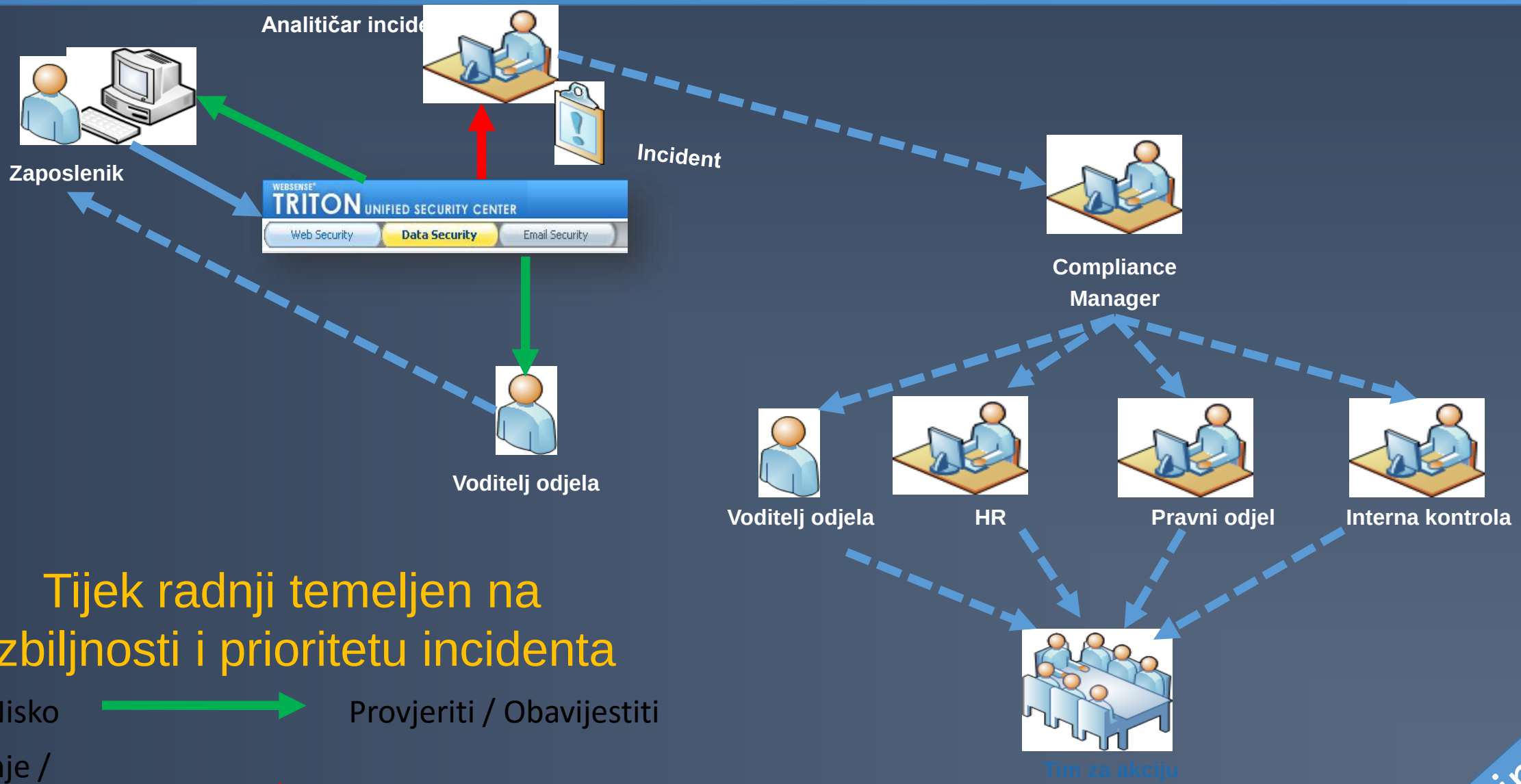
Regulations			STEP 1: Discuss General Data Types STEP 2: Relative Regulations (Wizard Avail) STEP 3: "ID" – Registered or Described STEP 4: Quantity or % for High Medium Low		IMPACT RATING LEGEND		
Breach Notification	HIPPA	PCI/ PCI-DSS			5 and 4	3 and 2	1
			Personal Identifiable Information	**ID**	**High**	**Moderate**	**Low**
			VIP PII	R	1	-	-
			PII	D	>100	> 25	> 2
			PHI	D	> 100	> 50	> 2
			Financial Information	**ID**	**High**	**Moderate**	**Low**
			Credit Cards	D	> 25	> 5	> 2
			Payroll Information	D	> 25	> 5	> 2
			Intellectual Property	**ID**	**High**	**Moderate**	**Low**
			Project X	R	> 25%	> 10%	10% <
			Design Document	R	> 25%	> 10%	10% <
			User name and Passwords	R	> 25%	> 10%	10% <

Korak 3: Definirajte prioritet reakcije

1. • Odaberite informaciju ili tip informacija koje ćete adresirati.
2. • Definirajte kanale koje ćete nadgledati.
3. • Odredite reakciju temeljenu na važnosti
4. • Navedite dodatne zahtjeve i akcije u slučaju postojanja istih.

Network Channels	High	Medium	Low	Notes
Web	Block/Alert	Block/Notify	Audit	Proxy to Block
Secure Web	Block/Alert	Block/Notify	Audit	SSL Inspection
Email	Block/Alert	Quarantine	Encrypt	Encryption
FTP	Block/Alert	Block/Notify	Audit	Proxy to Block
Network Printer	Block/Alert	Block/Audit	Audit	Install DLP Printer Agent
Mobile (Active Sync)	Block/Notify	Block	Audit	Install DLP for Mobile Proxy
Custom	Block	Block/Notify	Audit	TBD

Korak 4: Odredite tijek adresiranja incidenta



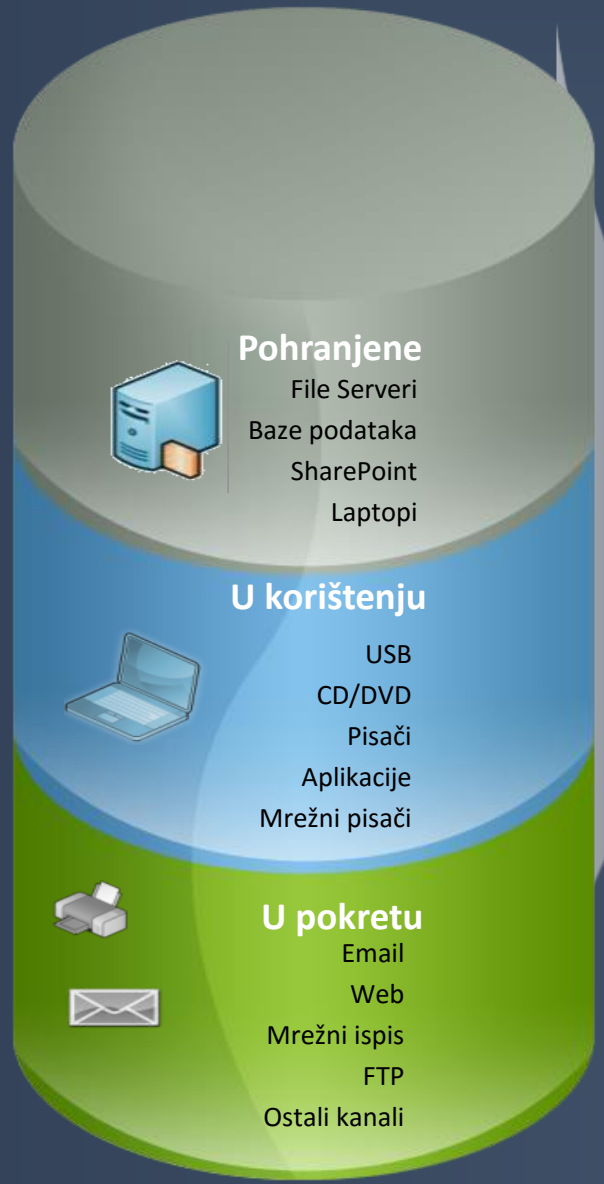
Tijek radnji temeljen na ozbiljnosti i prioritetu incidenta

Nisko → Provjeriti / Obavijestiti

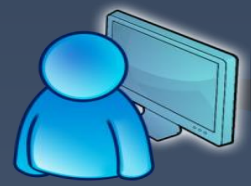
Srednje / Visoko → Zaustaviti / Istražiti

Primjer

Korak 5: Dodijelite jasne uloge i odgovornosti



Management & Reporting



Administrator

Incident Manager

Forenzičar

Auditor

Prava administratora

Neograničeni pristup, uključujući konfiguriranje, administraciju, podešavanja, incident managemt i reporting.

Prava Incident Mgr-a

Strogo kontrolirani pristup incidentu uz mogućnost izrade izvještaja.

Prava forenzičara

Detaljni pristup incidentu uz mogućnost izrade izvještaja.

Prava auditora

Samo uvid u specifične informacije (npr. PCI policies) bez mogućnosti pregleda forenzičkih detalja.

Korak 6: Framework za prvih 6 tjedana

1. Instaliranje i podešavanje
2. Nadgledanje mreže
3. Analiza rezultata
4. Prvi izvještaja upravi
5. Aktivnosti kontrole rizika
6. Analiza rezultata
7. Drugi izvještaj upravi

Cilj: Stvaranje uvida i postavljanje osnova projekta

FAZA I	PON	UTO	SRI	ČET	PET
Tjedan 1 – Install/Tune/Train					
Tjedan 2 – Nadgledanje					
Tjedan 3 – Analiza					
Tjedan 4 – Prvi izvještaj upravi			Izvještaj upravi		
Tjedan 5 – Kontrola rizika					
Tjedan 6 – Drugi izvještaj upravi					Izvještaj upravi

Korak 7: Proširite pokrivenost

1. Uključite nadgledanje Endpointa
2. Otkrijte nositelje i skenirajte podatke
3. Analiza rezultata
4. Treći izvještaj upravi
5. Aktivnosti kontrole rizika
6. Analiza rezultata
7. Četvrti izvještaj upravi

Cilj: Proširenje na Endpointe i početak otkrivanja podataka u IT infrastrukturi

FAZA II	PON	UTO	SRI	ČET	PET
Tjedan 7 – Uključivanje Endpointa					
Tjedan 8 – EP Nadgledanje / Podaci u mirovanju					
Tjedan 9 – EP Monitoring / Podaci u mirovanju					
Tjedan 10 – Treći izvještaj upravi			Izvještaj upravi		
Tjedan 11 – Kontrola rizika					
Tjedan 12 – Četvrti izvještaj upravi					Izvještaj upravi

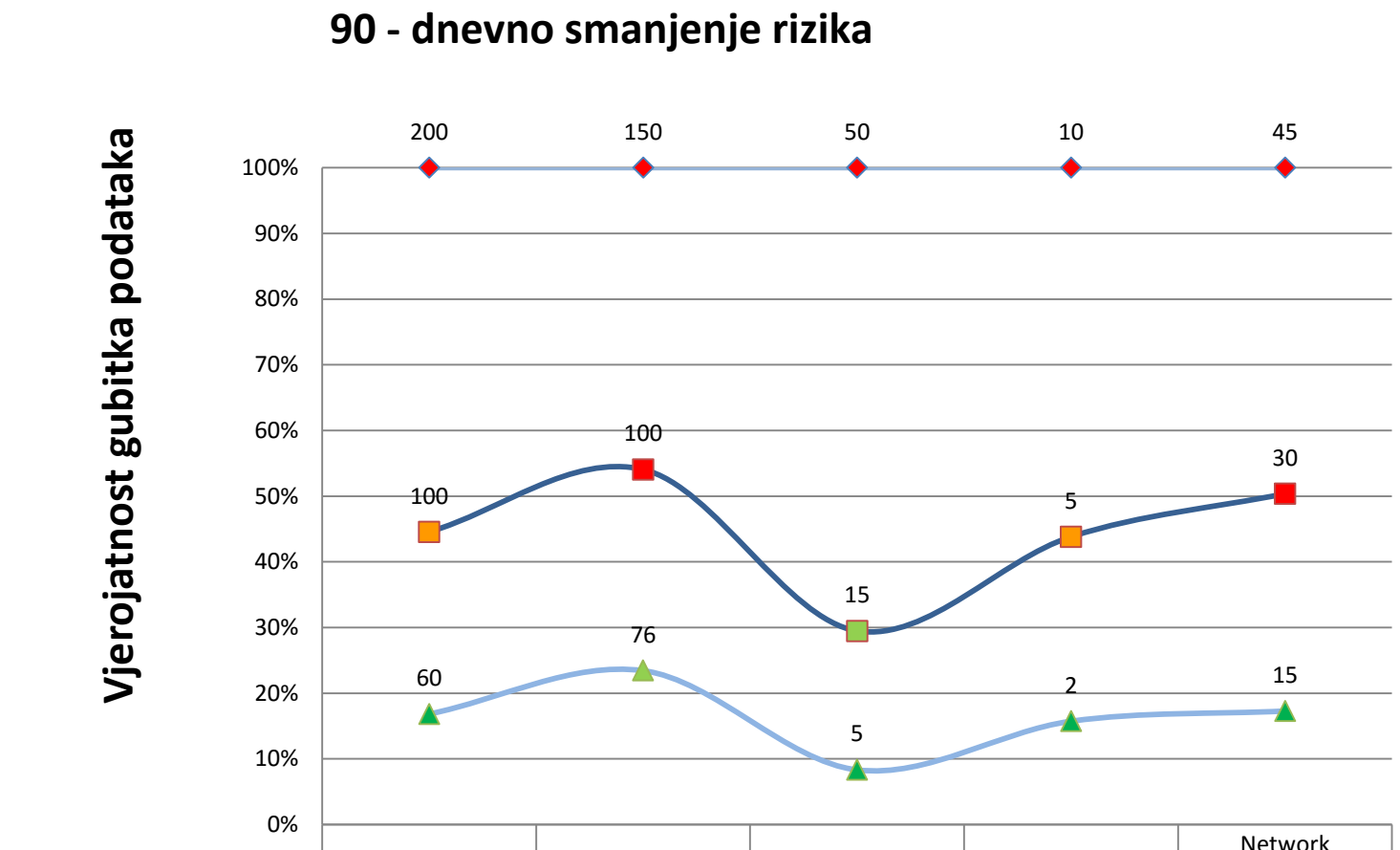
Korak 8: Konačna integracija

1. Stvaranje timova
2. Dodjeljivanje uloga
3. Trening
4. Pomaganje u odgovoru na incidente
5. Peti izvještaj upravi
6. Samostalno odgovaranje na incidente od strane timova (1)
7. Šesti izvještaj upravi

Cilj: Integriranje programa za zaštitu informacija u poslovanje

FAZA III	PON	UTO	SRI	ČET	PET
Tjedan 13 – Odabir & predstavljanje					
Tjedan 14 – Dodjeljivanje uloga					
Tjedan 15 – Trening uz pomoć pri odgovaranju na incidente					
Tjedan 16 – Peti izvještaj upravi			Izvještaj upravi		
Tjedan 17 – Timovi samostalno odgovaraju na incidente					
Tjedan 18 – Šesti izvještaj upravi					Izvještaj upravi

Korak 9: Pratite metriku smanjivanja rizika



	Web	Email	FTP	IM	Network Printing
Jan	200	150	50	10	45
Feb	100	100	15	5	30
Mar	60	76	5	2	15
90-Day Risk Reduction	70%	49%	90%	80%	67%

90-dnevno smanjenje rizika

GOALS	
30-dana	Osnova
60-dana	25%+ manje
90-dana	50%+ manje

LEGENDA
VISOKO
UMJERENO
NISKO
PRIHVATLJIVO

DLP ROI

Što nam vendori danas nude?

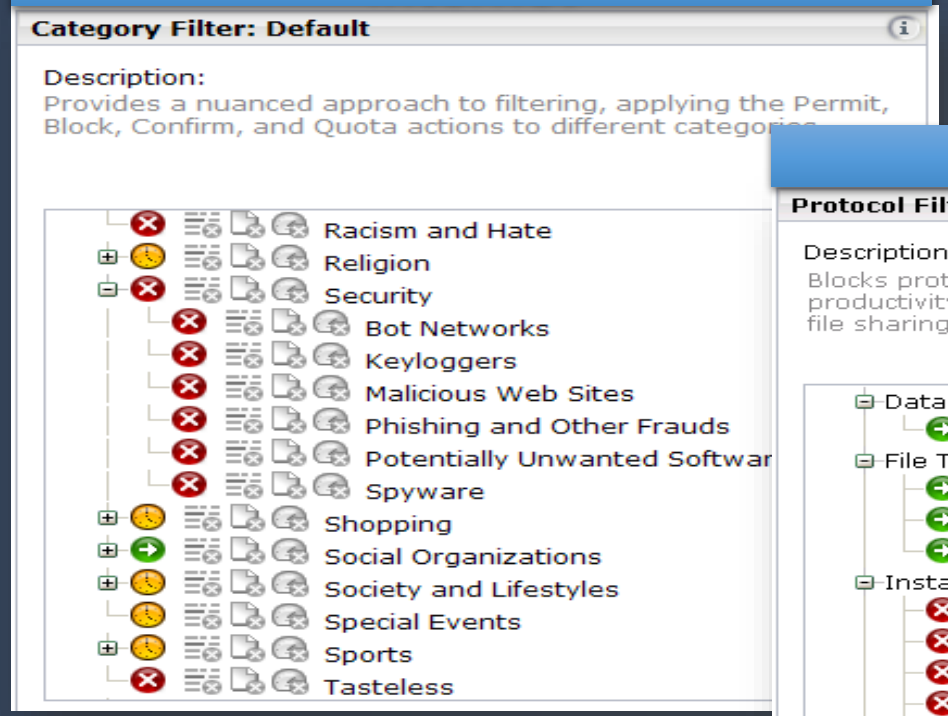
Jedinstvenu kontrolu sadržaja

U bilo kojoj kombinaciji

Uz korištenje jedinstvenog sučelja

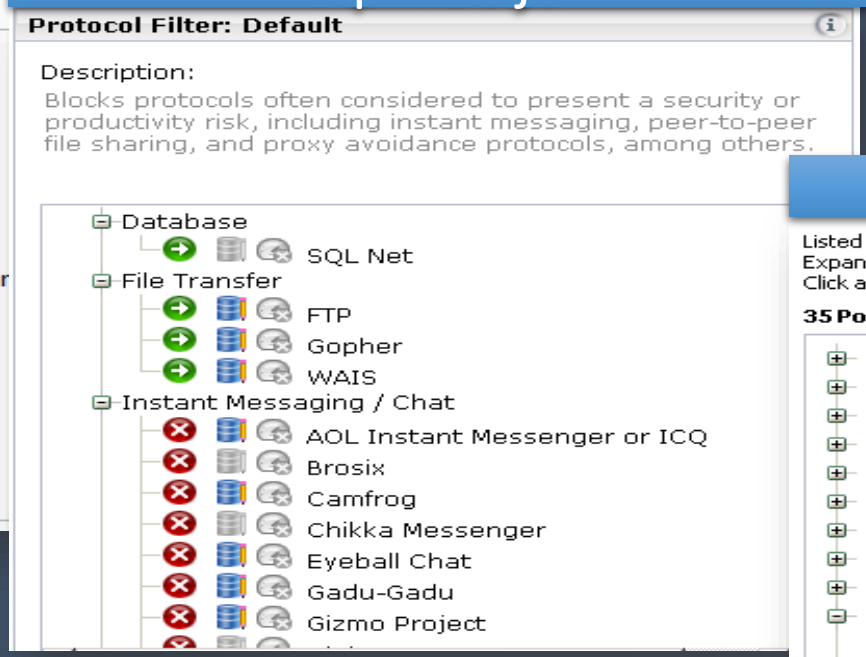
Zaštita, detekcija i kontrola

Internet



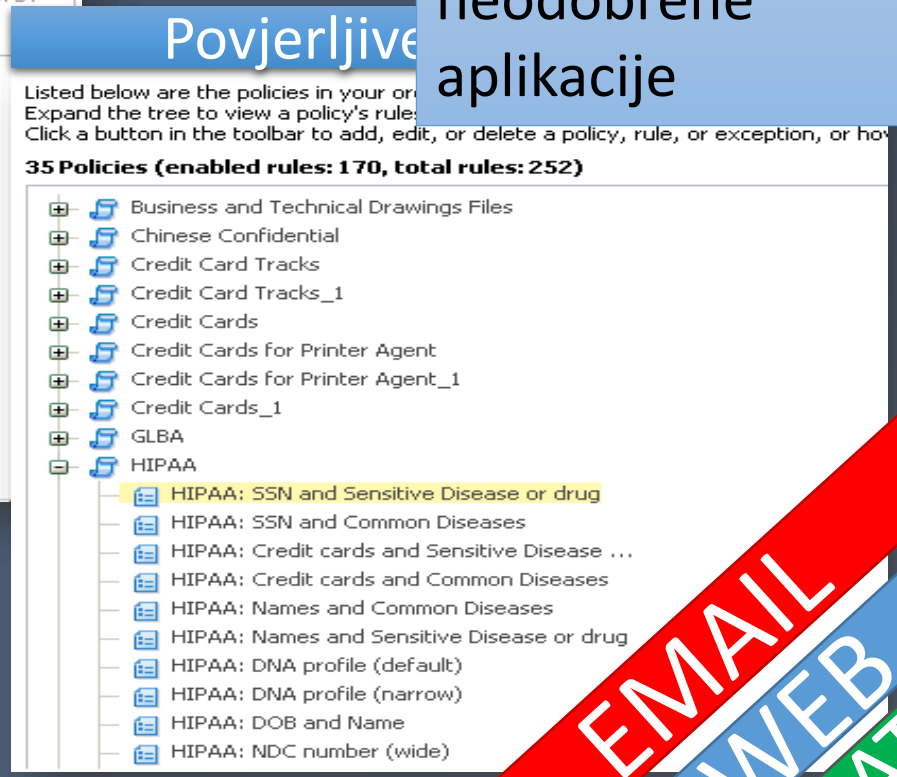
Smanjite izloženost prijetnjama.

Aplikacije



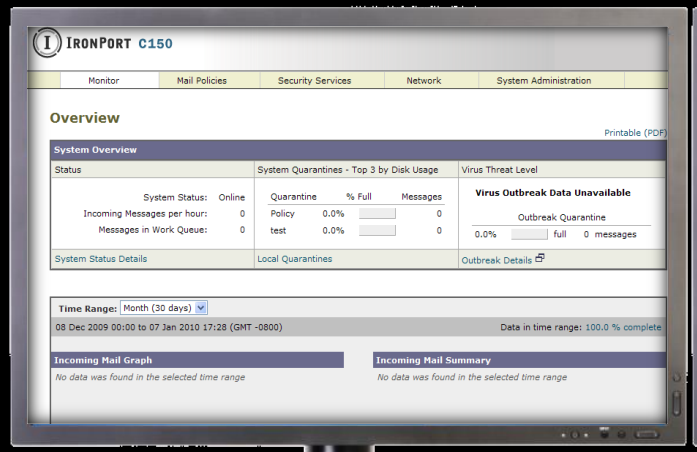
Proaktivno spriječite neodobrene aplikacije

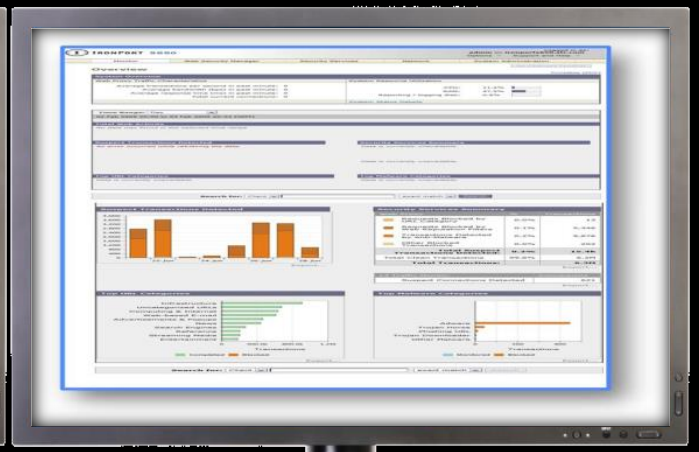
Povjerljive

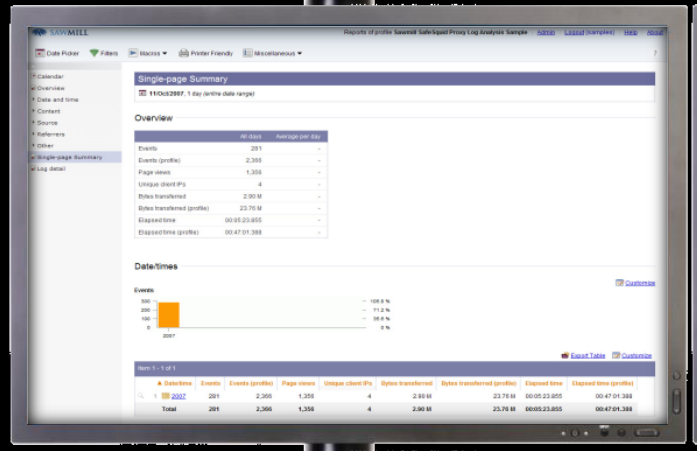


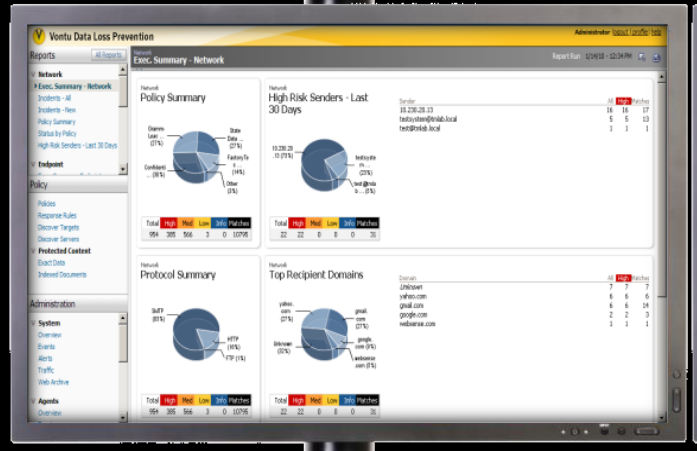
Kontrolirajte tijek informacija putem odobrenih kanala i aplikacija (npr: Chrome)

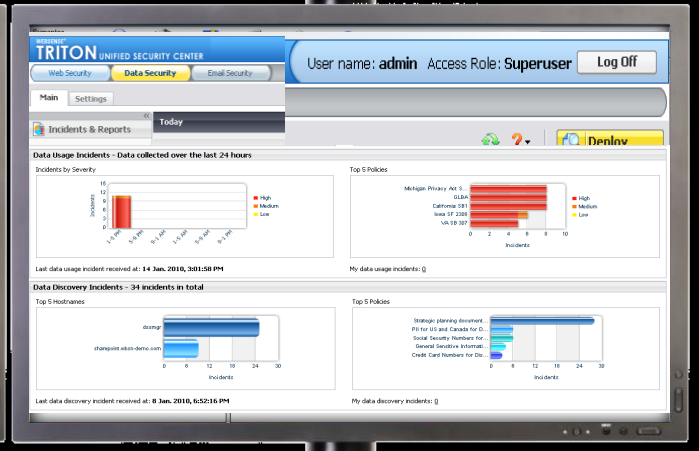
EMAIL
WEB
DATA











Imajte na umu ...

... Jednostavnost!

Prikaz najvažnijih vendora i rješenja

Symantec: najobuhvatnije DLP rješenje koje u potpunosti omogućava zaštitu informacija, bez obzira nalaze li se u cloudu, na mobilnim uređajima ili u vašim data centrima. Stručnjaci Symanteca su vodeći inovatori u DLP segmentu.

Digital Guardian: DLP Digital Guardiana vam daje najdetaljniji uvid i kontrole u usporedbi s drugim rješenjima na tržištu.

Forcepoint: rješenje koje nudi veliki broj funkcionalnosti “out-of-the box”, bez obzira koristi li se u cloudu ili on premise.

Intel Security: Total Protection for DLP štiti podatke korištenjem ePolicy Orchestrator-a uz kvalitetno riješene: deployment, management, updates i reporting.

Izvor, RSA konferencija, siječanj 2017: https://www.firecompass.com/blog/top-5-vendors-data-loss-prevention-dlp-technology-rsac-2017/

Prikaz najvažnijih vendora i rješenja

DLP, Gartner, 02/2017:

https://www.mpp.hr/app/download/15459061996/Gartner+Reprint%2C+DLP+Feb+2017.pdf?t=1513206194

Pitanja i odgovori

Kontakt podaci:

MIT POSLOVNI PROCESI D.O.O.
Matija Verić (CEO)
Milana Rešetara 40
HR-10000 Zagreb, Croatia
matija.veric@mpp.hr
+385 91 1321 059

VAŠ IT PARTNER OD POVJERENJA