POVERLJIVOST, INTEGRITET I DOSTUPNOST + DETEKCIJA

Predavač: dr Dušan Stefanović

OSNOVNI PRINCIPI BEZBEDNOSTI PODATAKA

POVERLJIVOST

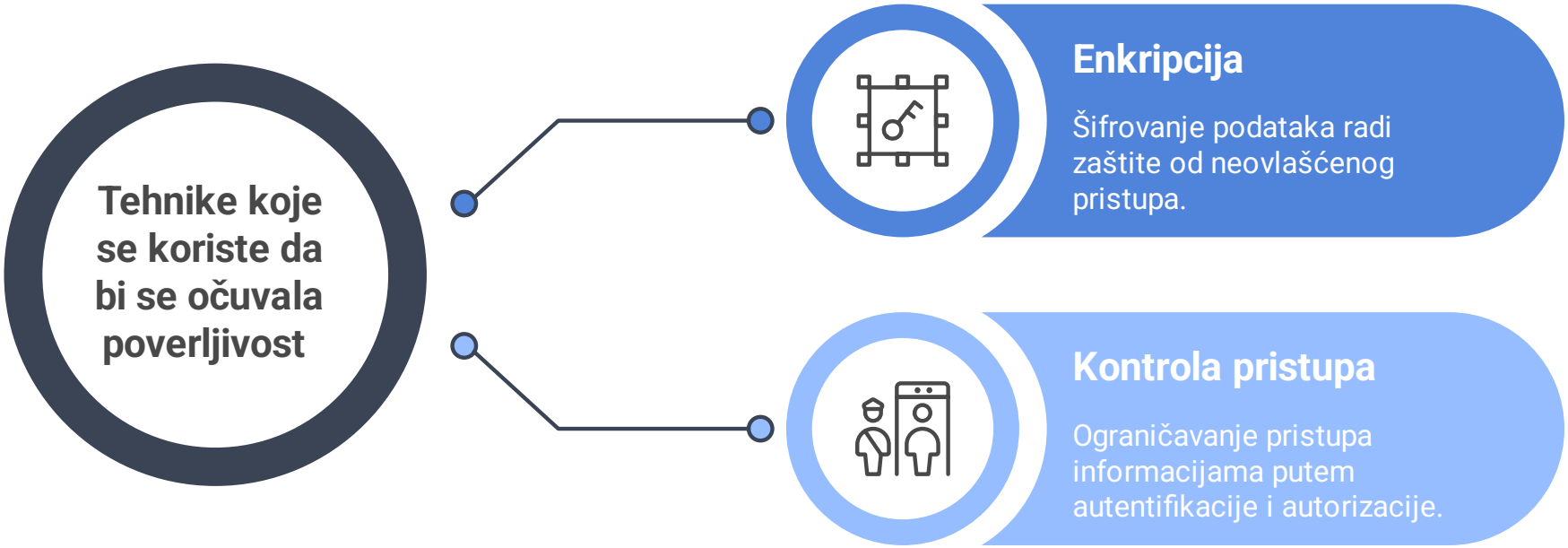
Poverljivost, integritet i dostupnost (CIA) su tri osnovna principa informacione bezbednosti

Ključni su za zaštitu **osetljivih informacija** i osiguravanje pravilnog funkcionisanja sistema i mreža.

POVERLJIVOST

Ovaj princip se fokusira na osiguravanje da informacije budu dostupne samo onima koji su ovlašćeni da ih pregledaju ili obrade.

Mere poverljivosti imaju za cilj sprečavanje neovlašćenog pristupa, otkrivanja ili curenja osetljivih podataka.



INTEGRITET

Uključuje konzistetnost, pouzdanost i ispravnost podataka kako bi se osiguralo da nisu izmenjeni od neovlašćenih osoba u toku njihovog životnog ciklusa.

Mere integriteta podataka koje pomažu u otkrivanju i sprečavanju neovlašćenih modifikacija su:

	Kontrolne sume	Digitalni potpis i MAC	Kontrola verzija
Opis	Otkrivanje neovlašćenih modifikacija podataka	Autentifikacija porekla i integriteta poruke	Praćenje i upravljanje promenama podataka
Funkcija	Izračunavanje vrednosti za verifikaciju integriteta podataka	Kriptografska tehnika za autentifikaciju	Sistem za beleženje promena tokom vremena
Korist	Jednostavno otkrivanje grešaka	Snažna autentifikacija i nemogućnost odbacivanja	Omogućava vraćanje i revizijske tragove

DOSTUPNOST

Osigurava da informacije i resursi budu dostupni i upotrebljivi kada su potrebni ovlašćenim korisnicima.

Ovaj princip uključuje sprečavanje ili umanjenje prekida usluga, sistema ili mreža, bilo da je reč o slučajnim kvarovima, prirodnim katastrofama ili zlonamernim napadima.

OSNOVNI PRINCIPI BEZBEDNOSTI PODATAKA

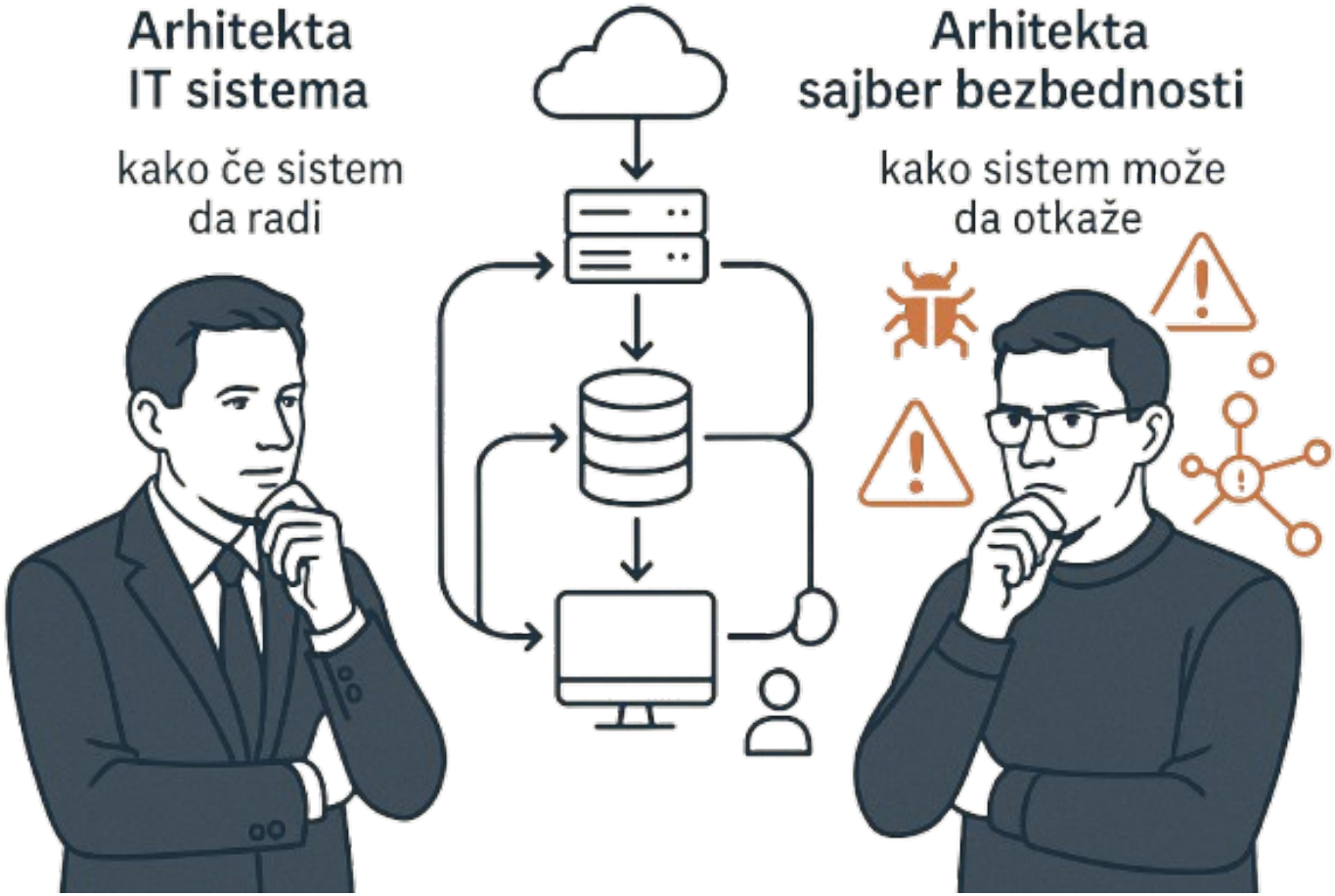
Dostupnost podataka
Garantuje neprekidan pristup podacima.

Poverljivost podataka
Osigurava da su osetljivi podaci dostupni samo autorizovanim korisnicima.

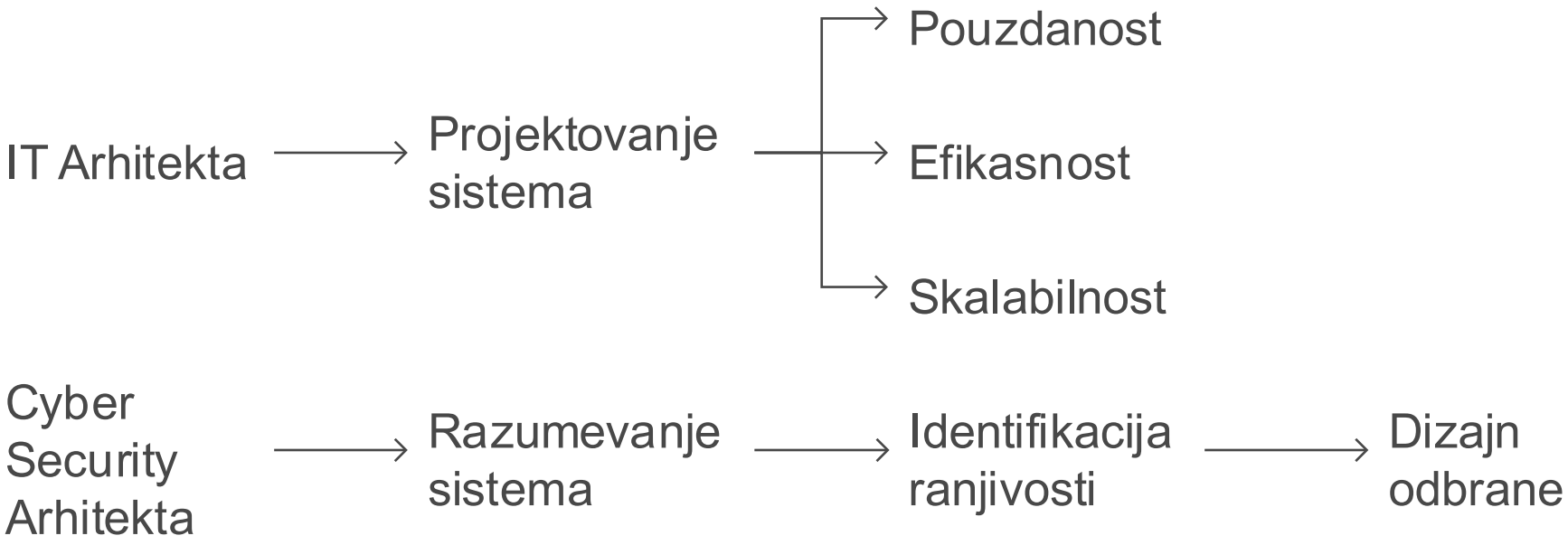
Integritet podataka
Održava tačnost i doslednost podataka.

CYBER SECURITY ARHITEKTA

“MINDSET“



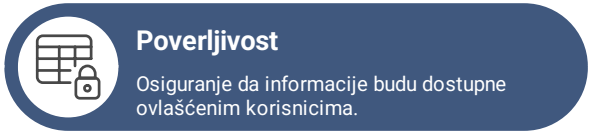
CYBER SECURITY ARHITEKTA

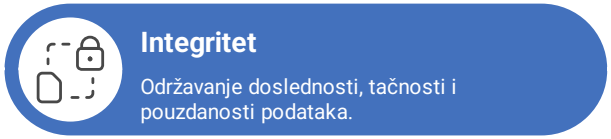


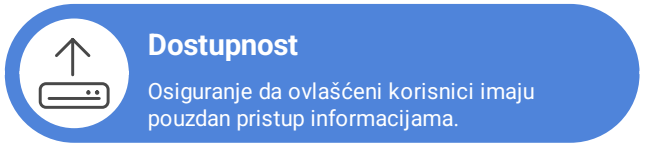
OSNOVE CYBER SECURITY ARHITEKTURE

Šta da uradimo da bi sistem bio bezbedan definišemo jednačinom:

Security = **Poverljivost** (Confidentiality) + **Integritet** (Integrity) + **Avaliability** (Dostupnost)

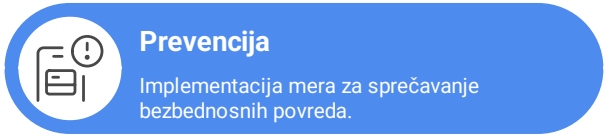


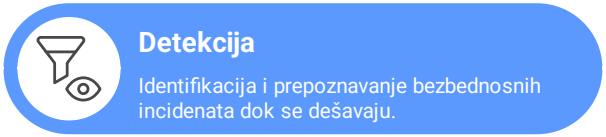


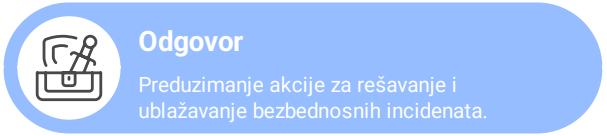


Kako da postignemo bezbednost definišemo jednačinom:

Security = **Prevencija** (Prevention) + **Detekcija** (Detection) + **Odgovor** (Response)







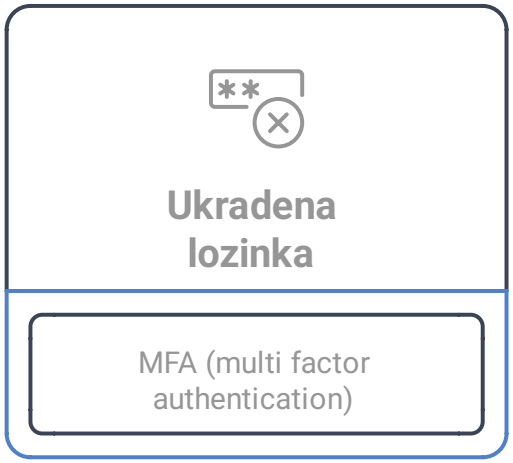
PREVENCIJA

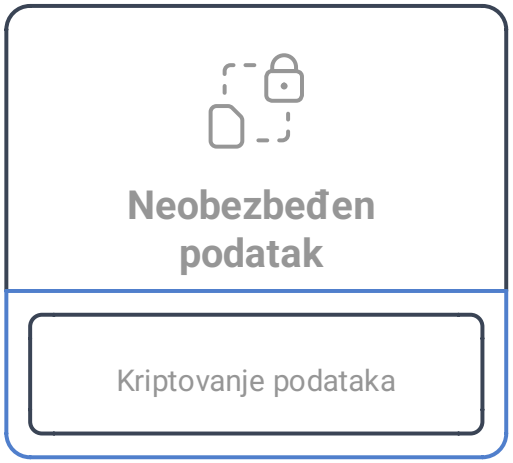
BOLJE SPREČITI NEGO LEČITI

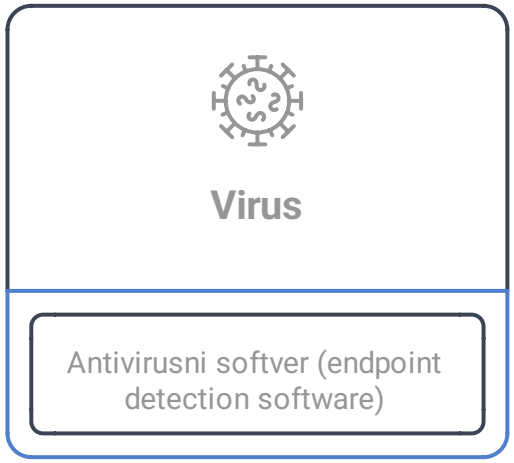
STRATEGIJA ODVRAĆANJA

PREVENCIJA U IT SISTEMIMA

Gde sve može da se javi *sajber* proboj?

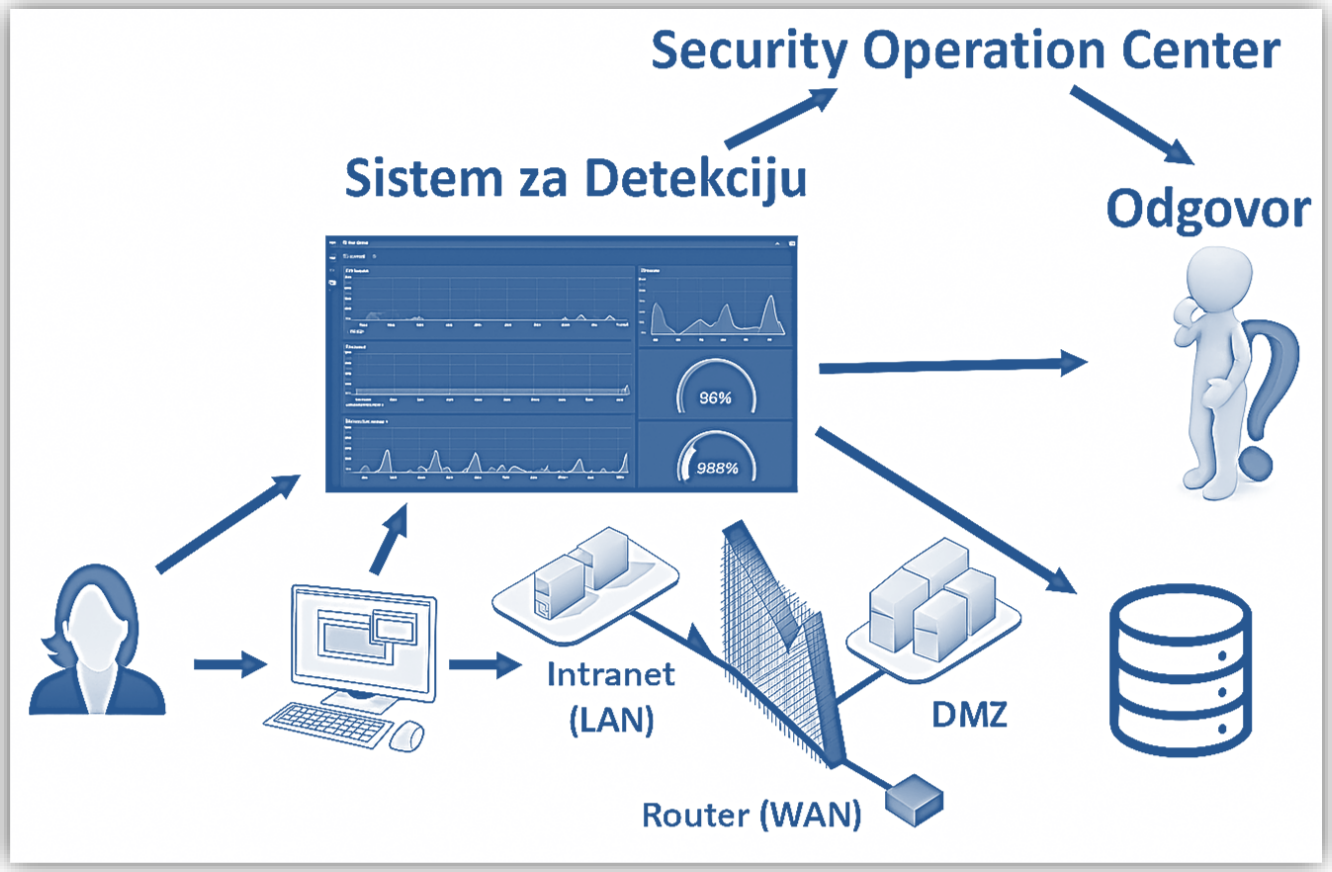






DETEKCIJA

Detekcija se zasniva na praćenju i sakupljanju informacija sa svakog nivo zaštite u centralizovani security managment sistem



DETEKCIJA

Četiri ključna stuba detekcije u okviru bezbednosne arhitekture su:

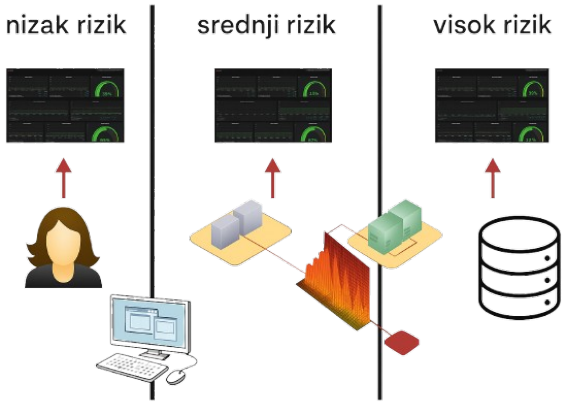
Tehnologije koje se koriste za ovakvu vrstu detekcije su:

- SIEM (Security information and event managment system)
- XDR (Extended detection and response system)

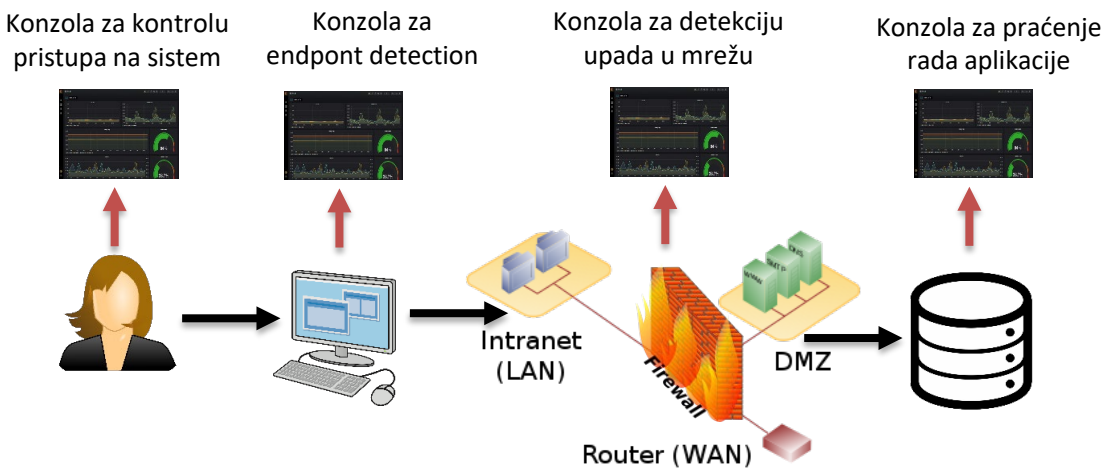
DETEKCIJA

TRADICIONALNI PRISTUP

Slojevi (nivoi) zaštite



Svaki nivo zaštite je izvor security informacija

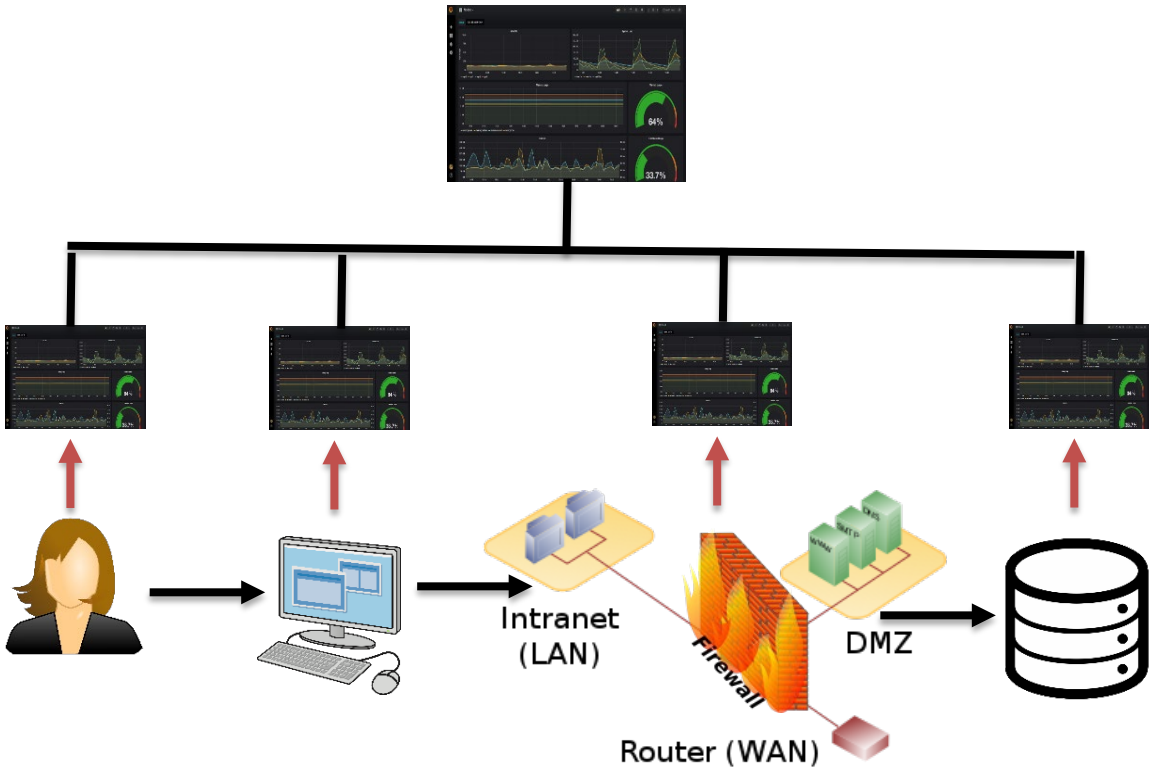


Detekcija je na svakom nivou zaštite nezavisna, složena za praćenje i ne postoji konzistentan pogled na incidente.

Rezultat toga je da se aktiviraju alarmi na različitim nivoima odbrane a da se pritom radi o istom napadu.

TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

SECURITY INFORMATION AND EVENT MANAGMENT SYSTEM



TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

OSOBINE SIEM SISTEMA

Prikupljanje podataka

Prikupljanje informacija iz različitih izvora (alarme, log zapisi i tok podataka)

Korelacija

Pronalaženje veza između podataka sakupljenih iz različitih bezbednosnih slojeva

Analitika

Na osnovu sakupljenih podataka se primenjuje analitika

Analiza podataka

Razumevanje i tumačenje podataka

1. Kompleksna pravila i polise (da li su se desili događaji koji ispunjavaju kriterijume) – znamo šta tražimo
2. Anomalije (prikaz netipičnog ponašanja) – ne znamo šta tražimo
3. Trend (kreiranje izveštaja koji pokazuju statistiku npr. broj aktiviranih alarma,vrste alarma, vreme odogovora.

ALATI ZA DETEKCIJU I REAGOVANJE NA SAJBER INCIDENTE (SIEM PLATFORME)

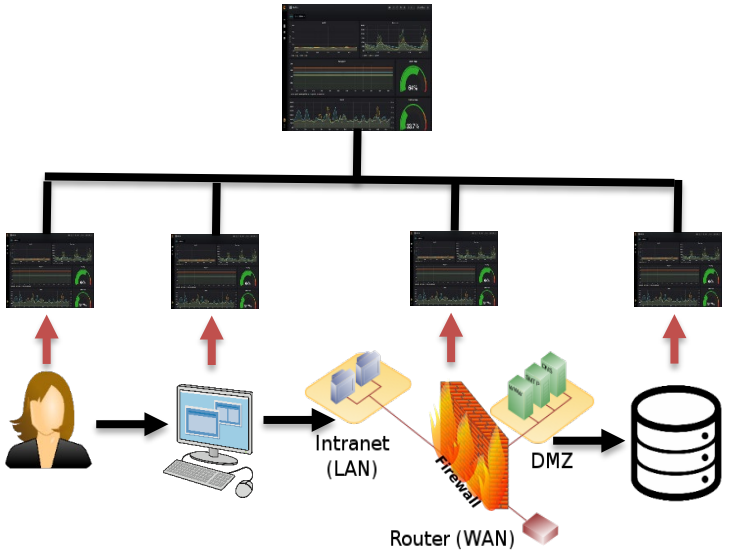
	Splunk Enterprise Security	IBM QRadar	LogRhythm	Cisco SecureX	RSA NetWitness	Fortinet FortiSIEM
Detekcija pretnji	Napredna analiza podataka i vizualizacija	Analiza logova i detekcija pretnji	Analiza logova i analiza ponašanja	Analiza logova i detekcija pretnji	Analiza logova i detekcija pretnji	Analiza logova i detekcija pretnji
Analiza podataka	Napredna analiza podataka i vizualizacija	Napredne funkcije za analizu podataka	Veštačka inteligencija i mašinsko učenje	Integracija analize logova	Napredna analiza podataka	Kombinacija analize logova
Upravljanje incidentima	Identifikacija i istraživanje sigurnosnih pretnji	Detekcija pretnji i upravljanje incidentima	Kombinacija analize logova, detekcija pretnji	Automatizacija odgovora na incidente	Forenzička analiza	Automatizacija odgovora na incidente

TEHNOLOGIJE ZA DETEKCIJU INCIDENATA
EXTENDED DETECTION AND RESPONSE

Endpoint Detection and Response (EDR) je tip sigurnosne tehnologije koja se fokusira na zaštitu i odgovor na pretnje na nivou krajnjih tačaka (endpointa) u mreži.

Endpointi uključuju uređaje poput:

- računara
- servera
- mobilnih uređaja
- drugih IoT uredjaja koji su povezani sa mrežom i imaju potencijal da budu cilj napada.

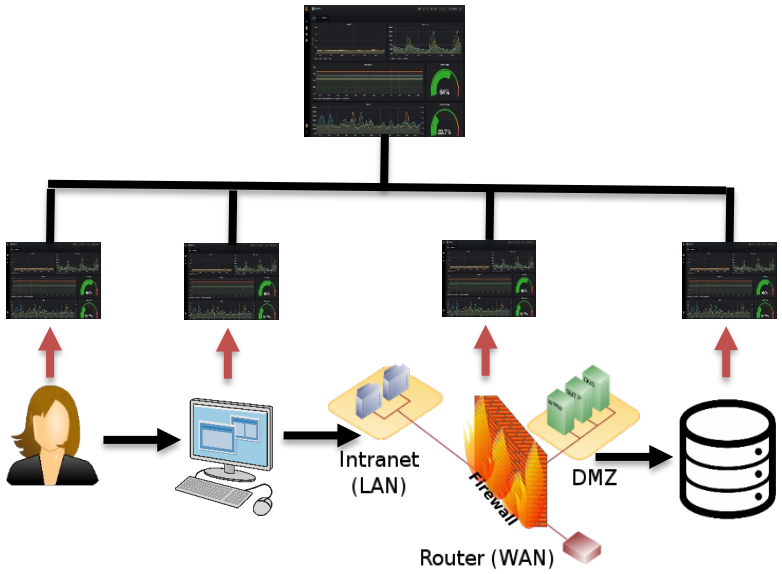


TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

EXTENDED DETECTION AND RESPONSE

Osnovnii cilj EDR tehnologije je da pruži detaljan uvid u aktivnosti koje se dešavaju na endpointima kako bi se otkrile i sprečile pretnje.

Tehnologija prati **ponašanje fajlova**, **procesa**, **mrežnog saobraćaja** i drugih aktivnosti na uređajima kako bi identifikovala neobične ili sumnjive aktivnosti koje mogu ukazivati na napad.



KARAKTERISTIKE EDR SISTEMA

Detekcija pretnji

Praćenje i analiza aktivnosti na endpointima radi identifikacije potencijalno zlonamernih aktivnosti.

Analiza ponašanja

Upotreba naprednih tehnika analize ponašanja kako bi se identifikovale anomalije i neobični obrasci aktivnosti koji mogu ukazivati na pretnje.

Odgovor na incidente

Mogućnost brzog odgovora na pretnje, uključujući izolaciju zaraženih uređaja, blokiranje zlonamernih aktivnosti i sprovođenje forenzičke analize.

Izveštavanje i monitoring

Praćenje sigurnosnih događaja na endpointima i generisanje izveštaja o pretnjama i incidentima.

Integracija sa drugim alatima

Mogućnost integrisanja sa drugim sigurnosnim alatima i platformama kako bi se obezbedila celovita sigurnosna strategija.

KLJUČNE KOMPONENTE EDR SISTEMA

Upozorenje na konzoli
Centralizovana konzola za upozorenja, logove i izveštaje o incidentima.

Osnovna funkcionalnost EDR-a
Osnovne funkcije: prikupljanje podataka sa krajnjih tačaka, detekcija ponašanja i automatske reakcije.

EPP paket
Integracija sa klasičnim antivirusnim i anti-malware alatima.

Prevencija
Mehanizmi prevencije: blokiranje poznatih pretnji, mitigacija exploit-a itd.

Integracija sa trećim stranama
Mogućnost integracije sa drugim sigurnosnim alatima: SIEM, SOAR, izvori obaveštajnih pretnji.

EDR napredna reakcija
Napredne opcije reagovanja: izolacija uređaja, obustavljanje procesa i forenzičke analize.

Geografska podrška
Globalna pokrivenost i sposobnost prilagođavanja različitim pravnim/regulatornim okvirima.

Upravljane usluge
Pružanje EDR funkcionalnosti putem MSSP partnera.

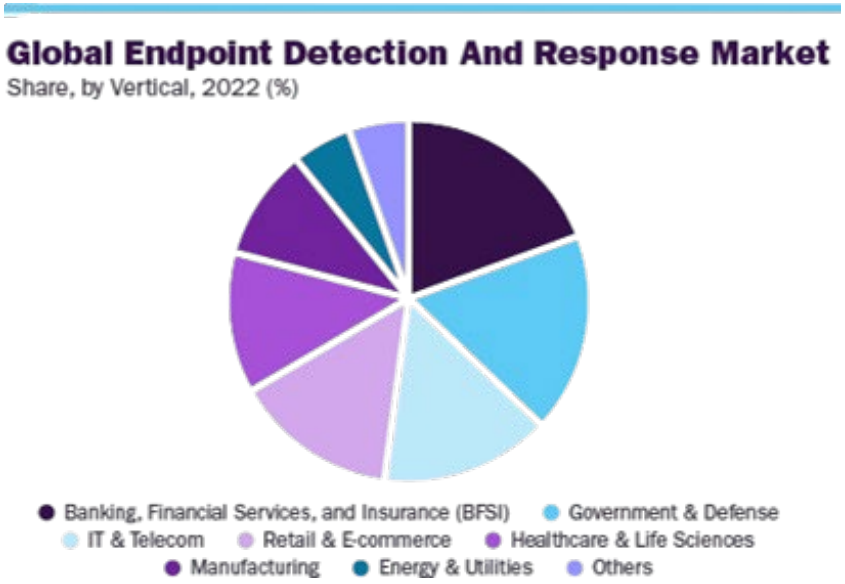
Podrška za operativne sisteme
Podrška za različite operativne sisteme (Windows, Linux, macOS itd.).

PLATFORME ZA DETEKCIJU INCIDENATA EXTENDED DETECTION AND RESPONSE

	CrowdStrike Falcon	Carbon Black	Microsoft Defender	Symantec EDR	Trend Micro Apex One	SentinelOne	FireEye HX	Bitdefender GravityZone
Detekcija pretnji	Napredna detekcija pretnji	Napredna analiza ponašanja	Integrisana detekcija pretnji	Detekcija pretnji kombinovana	Sveobuhvatna detekcija pretnji	Detekcija zasnovana na veštačkoj inteligenciji	Detekcija pretnji kombinovana	Detekcija zasnovana na veštačkoj inteligenciji
Analiza ponašanja	Da	Da	Da	Da	Da	Da	Da	Da
Odgovor na incidente	Da	Da	Da	Da	Da	Da	Da	Da
Dodatne funkcije	Na nivou krajnje tačke	Deo VMware-a	Integrisano rešenje	Detekcija pretnji	Antivirusna zaštita	Koristi veštačku inteligenciju, mašinsko učenje	Istraživanje incidenata	Koristi veštačku inteligenciju

UDEO EDR TRŽIŠTA PO SEKTORIMA U 2022.

Sektor	Udeo (%)
Bankarstvo, finansije i osiguranje (BFSI)	22%
Državni sektor i odbrana	15%
IT i telekomunikacije	18%
Maloprodaja i e-trgovina	12%
Zdravstvo i biološke nauke	10%
Proizvodnja	8%
Energija i komunalne usluge	7%
Ostali sektori	8%



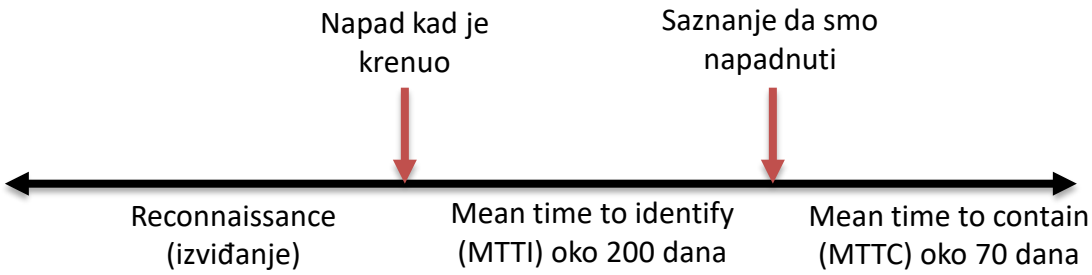
TEHNOLOGIJE ZA DETEKCIJU INCIDENATA
EDR + SIEM

EDR i SIEM se koriste za različite svrhe i fokusiraju na različite aspekte detekcije i odgovora na pretnje.

U mnogim slučajevima, organizacije koriste i EDR i SIEM tehnologije zajedno kako bi dobile sveobuhvatan pristup detekciji i odgovoru na pretnje, koristeći EDR za zaštitu krajnjih tačaka i SIEM za centralizovanu analizu i upravljanje sigurnosnim događajima na nivou cele organizacije.

OSNOVE CYBER SECURITY

Traženje (Hunt)



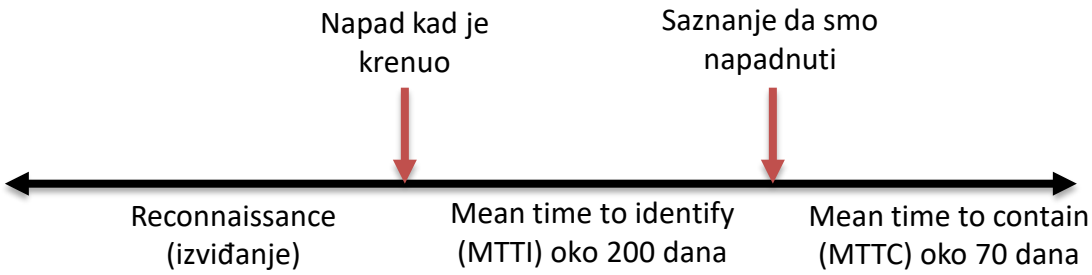
Mean time to identify je prosečno vreme koje protekne od trenutka napada do trenutka kada je kompanija svesna da je napadnuta i iznosi oko 200 dana

Kratak MTTI znači brzo otkrivanje napada i manji potencijalni gubici.

Dug MTTI ukazuje na **slabosti u monitoringu**, **SIEM sistemima** ili **obuci osoblja**.

OSNOVE CYBER SECURITY

Traženje (Hunt)



Mean Time to Contain (MTTC) označava prosečno vreme koje je potrebno organizaciji da **izoluje i obuzda bezbednosni incident** nakon što je detektovan.

To je ključna metrika u **incident response** procesu, jer meri efikasnost tima u **sprečavanju širenja pretnje** unutar IT infrastrukture.

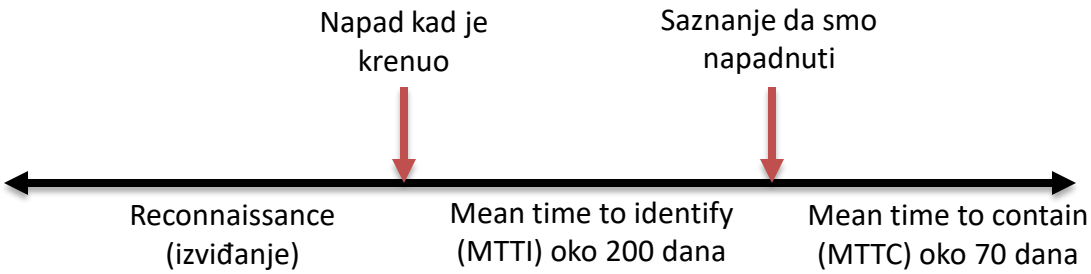
MTTC = Ukupno vreme do kontrole svih incidenata / Broj incidenata

Mean time to contain je prosečno vreme koje protekne od trenutka kada je kompanija svesna da je napadnuta do trenutka da je napad uklonjen iznosi **70 dana**.

OSNOVE CYBER SECURITY

Traženje (Hunt)

Cilj je da **skaratimo vreme saznanja da se napad dogodio** tj. MTTI a to se postiže lovom na pretnje **(Threat Hunting)**



Lov na pretnje se bazira na proaktivnost cyber security analitičara jer se napad još nije desio tj. nije otkriven kao što se nisu sistemi za detekciju tj. alarmi se aktivirali

Lov se zasniva na iskustvu i instiktu analitičara

TESTIRANJE PREĐENOG GRADIVA

Koja su tri osnovna principa informaciono-bezbednosnog modela CIA?

a) Privatnost, pouzdanost, efikasnost

b) Poverljivost, integritet, dostupnost

c) Sigurnost, otkrivanje, odbrana

d) Praćenje, upravljanje, zatvaranje

TESTIRANJE PREĐENOG GRADIVA

Koji princip CIA modela se odnosi na zaštitu od neovlašćenog pristupa podacima?

a) Integritet

b) Dostupnost

c) Poverljivost

d) Praćenje

TESTIRANJE PREĐENOG GRADIVA

Kako se zove proaktivan proces u kome analitičari traže znake napada pre nego što se on otkrije sistemski?

a) Penetration Testing

b) Threat Hunting

c) SIEM analiza

d) Forenzička obrada

TESTIRANJE PREĐENOG GRADIVA

Koji sistem omogućava centralizovanu obradu bezbednosnih događaja u organizaciji?

a) EDR

b) IDS

c) SIEM

d) VPN

TESTIRANJE PREĐENOG GRADIVA

Koji parametar meri prosečno vreme od početka napada do njegovog otkrivanja?

a) MTTI

b) MTTD

c) MTTF

d) MTTR

TEME ZA ISTRAŽIVAČKI RAD

1. **Poređenje SIEM i EDR tehnologija – prednosti i mane**
2. **Uloga prevencije i detekcije u savremenim sajber napadima**
3. **Kako skraćenje MTTI i MTTC može spasiti infrastrukturu**
4. **Analiza uspešnosti threat hunting strategija u velikim organizacijama**
5. **Simulacija napada i primena SIEM sistema za analizu događaja**
6. **Značaj dostupnosti (Availability) u cloud okruženjima**
7. **Studija slučaja: Kako je upotreba SIEM-a pomogla u sprečavanju stvarnog napada**

ŠABLON ZA PISANJE ISTRŽIVAČKOG RADA

Naslov

Unesite jasan i informativan naslov koji precizno opisuje temu rada.

Uvod

Predstavite temu rada, njenu važnost i istraživačko pitanje. Formulišite cilj rada.

Pregled literature

Opišite prethodna istraživanja i relevantne izvore koji se odnose na vašu temu.

Metodologija

Objasnite korišćene metode istraživanja: kvalitativne, kvantitativne, studije slučaja itd.

Rezultati

Prikažite rezultate istraživanja (numerički, tabelarno, grafički – po potrebi).

Diskusija

Prokomentarišite rezultate, uporedite ih sa prethodnim istraživanjima i diskutujte o njihovom značaju.

Zaključak

Sažmite glavne nalaze, potvrdite ili odbacite hipotezu i predložite pravce za dalja istraživanja.

Reference

Navedite sve korišćene izvore u odgovarajućem formatu.

Dodaci

Po potrebi dodajte dodatne materijale: upitnike, grafikone, sirove podatke itd.