POVERLJIVOST, INTEGRITET I DOSTUPNOST + DETEKCIJA

Predmet: Zaštita podataka u komunikacionim mrežama

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.

Tehnike koje se koriste da bi se očuvala poverljivost su:

- **Enkripcija**
- **kontrola pristupa** (autentifikacija i autorizacija)

OSNOVNI PRINCIPI BEZBEDNOSTI PODATAKA

INTEGRITET

Integritet:

Odnosi na pouzdanost i tačnost informacija tokom njihovog životnog ciklusa.

Uključuje konzistetnost, pouzdanost i ispravnost podataka kako bi se osiguralo da nisu izmenjeni od neovlašćenih osoba.

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

- **Kontrolne sume (checksums)**
- **Digitalni potpis i MAC (Message Authentication Code)**
- **Kontrole verzija**

OSNOVNI PRINCIPI BEZBEDNOSTI PODATAKA

DOSTUPNOST

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.

Kako bi se minimiziralo vreme nedostupnosti i osiguralo neprekidno funkcionisanje mere dostupnosti uključuju:

- **Redundansu**
- **Toleranciju na greške**
- **Planiranje oporavka od katastrofe**
- **Dizajn robustne infrastrukture**

OSNOVNI PRINCIPI BEZBEDNOSTI PODATAKA

Prilikom projektovanja informacionog sistema potrebno je sagledati:

1. Da li su ispunjemi zahtevi koji se odnose na poverljivost podataka tj. da li su osetljivi podaci dostupni samo osobama koje su autorizovane?
2. Da li sistem ima mehanizme provere integriteta podataka?
3. Da li su podaci neprekidno dostupni?

CYBER SECURITY ARHITEKTA

MINDSET

Arhitekta IT Sistema brine o tome kako će sistem da radi

Cyber Security arhitekta razmišlja kako sistem može da otkaže

- Mora prvo da razume kako sistem radi da bi znao kako može da otkaže

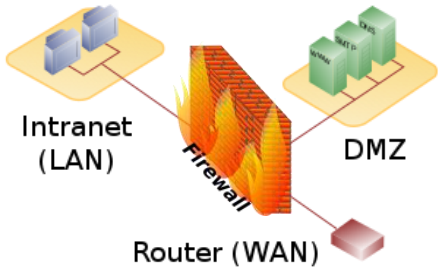
Šta može da bude security problem?
Ukradena lozinka…

Rešenje:
MFA (multi factor auth)

Šta može da bude security problem?
Virus…

Rešenje:
Antivirusni softver (endpoint detection software)

Šta može da bude security problem?
DDOS napad sa Interneta,...



Rešenje:
Firewall

Šta može da bude security problem?
Neobezbeđen podatak

Rešenje:
Kripcija podataka

OSNOVE CYBER SECURITY ARHITEKTURE

Šta želimo da uradimo definišemo sledećom jednačinom:

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

Kako želimo da postignemo veću bezbednost definišemo sledećom jednačinom:

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

OSNOVE CYBER SECURITY ARHITEKTURE

PREVENCIJA

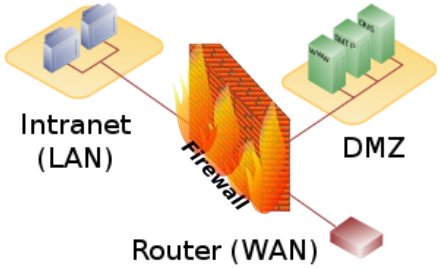
Šta može da bude security problem?
Ukradena lozinka…

Rešenje:
MFA (multi factor auth)

Šta može da bude security problem?
Virus…

Rešenje:
Antivirusni softver (endpoint detection software)

Šta može da bude security problem?
DDOS napad sa Interneta,...



Rešenje:
Firewall

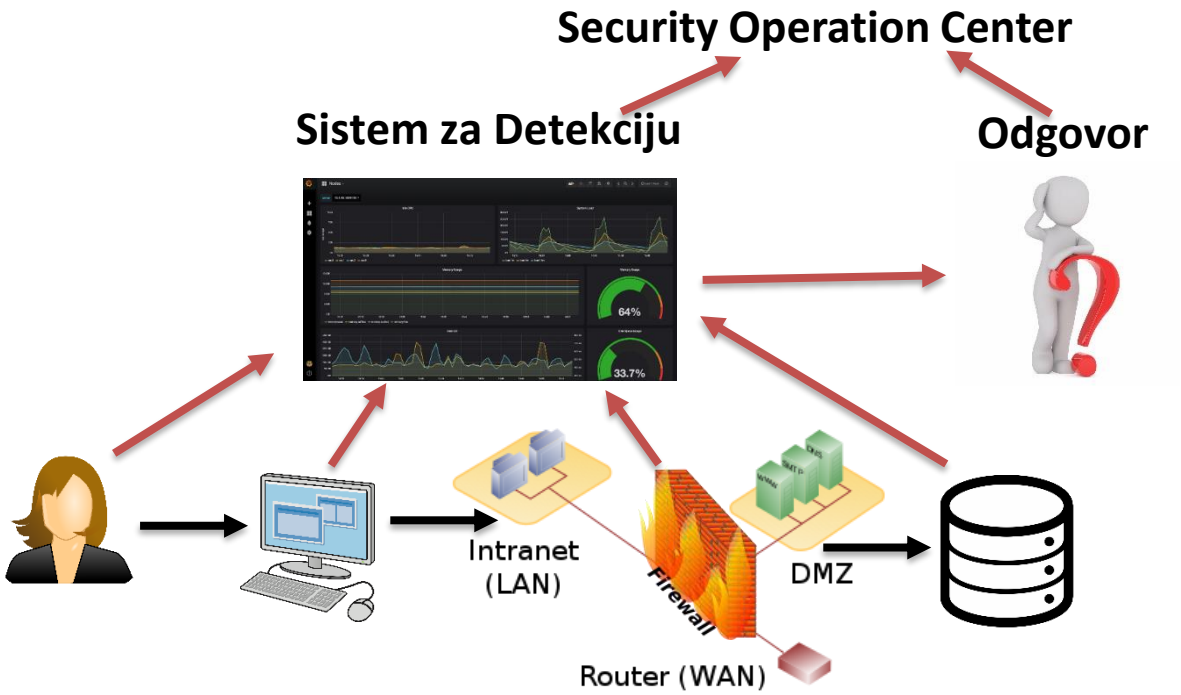
Šta može da bude security problem?
Neobezbeđen podatak

Rešenje:
Kripcija podataka

OSNOVE CYBER SECURITY ARHITEKTURE

DETEKCIJA

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



OSNOVE CYBER SECURITY ARHITEKTURE

DETEKCIJA

Detekcija uključuje:

Praćenje (Monitor)

Analizu (Analyze)

Izveštavanje (Report)

Traženje (Hunt)

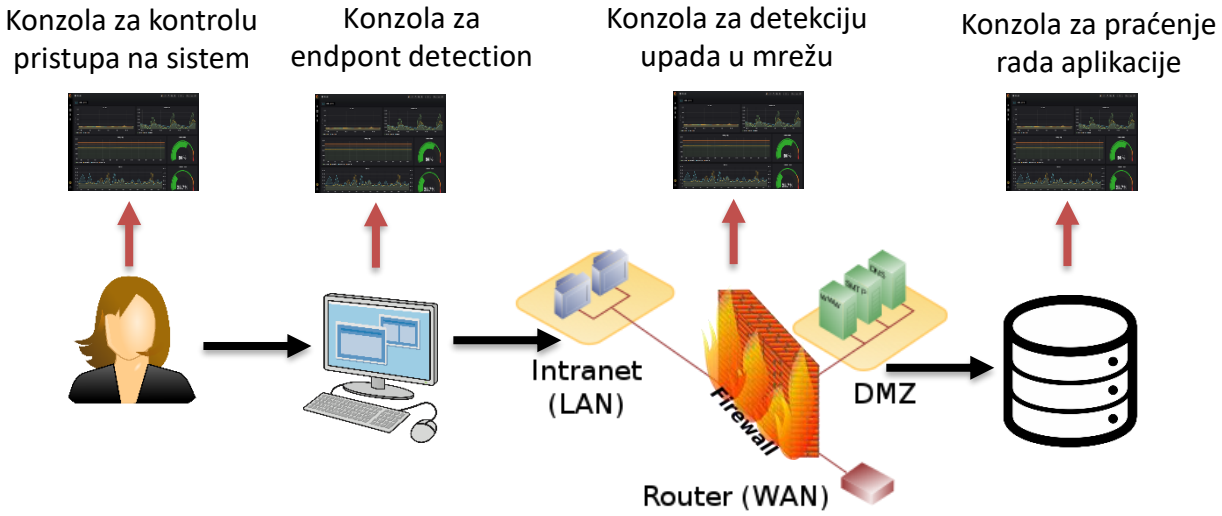
Tehnologije koje se koriste za ovakvu vrstu detekcije su:

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

DETEKCIJA

TRADICIONALNI PRISTUP

Svaki nivo zaštite je izvor security informacija



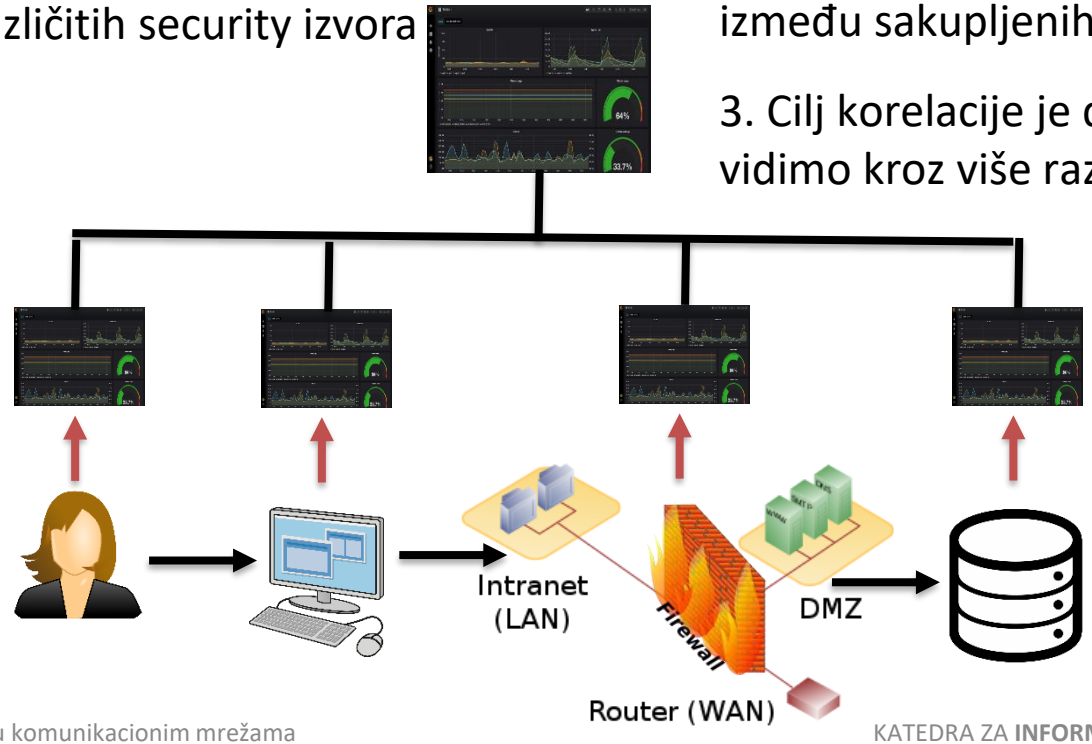
Problem je što je detekcija na svakom nivou zaštite nezavisna, složena za praćenje i ne postoji konzistentan pogled na incidente.

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

1. SIEM je baza koja sakuplja informacije (**alarme, log zapisi i tok podataka**) sa različitih security izvora



2. SIEM na osnovu sakupljenih podataka primenjuje analitiku i **traži korelacije** između sakupljenih podataka

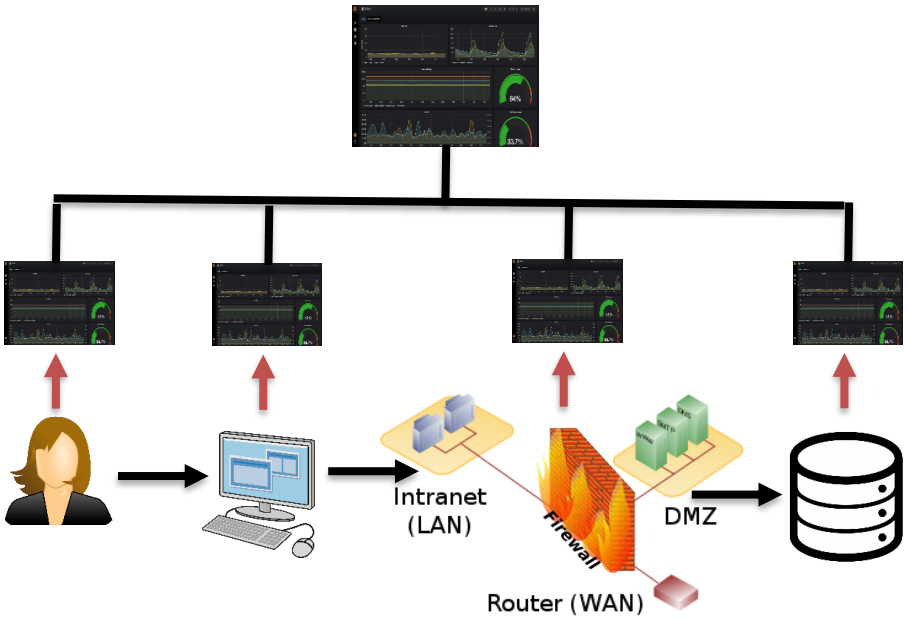
3. Cilj korelacije je da jedan napad ne vidimo kroz više različitih alarma

TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

SECURITY INFORMATION AND EVENT MANAGMENT SYSTEM

4. Analiza podataka

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



TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

SECURITY INFORMATION AND EVENT MANAGMENT SYSTEM

Splunk Enterprise Security:

Splunk je jedan od lidera na tržištu SIEM tehnologija. Splunk Enterprise Security pruža **napredne mogućnosti analize podataka i vizualizacije** kako bi se identifikovale i istražile sigurnosne pretnje.

IBM QRadar:

QRadar je SIEM platforma kompanije IBM koja kombinuje **analizu logova, detekciju pretnji i upravljanje incidentima**. Pruža napredne funkcije za analizu podataka i identifikaciju sigurnosnih rizika.

LogRhythm:

LogRhythm pruža SIEM rešenje koje kombinuje **analizu logova, detekciju pretnji i analizu ponašanja**. Ova platforma koristi **veštačku inteligenciju i mašinsko učenje** za identifikaciju sumnjivih aktivnosti.

TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

SECURITY INFORMATION AND EVENT MANAGMENT SYSTEM

Cisco SecureX:

SecureX je SIEM platforma kompanije Cisco koja integriše analizu logova, detekciju pretnji i automatizaciju odgovora na incidente. Pruža celovit pregled nad sigurnosnim događajima u mrežnoj infrastrukturi.

RSA NetWitness:

NetWitness je SIEM platforma kompanije RSA koja kombinuje analizu logova, detekciju pretnji i forenzičku analizu. Pruža dublji uvid u sigurnosne događaje kroz naprednu analizu podataka.

Fortinet FortiSIEM:

FortiSIEM je SIEM platforma koja kombinuje analizu logova, detekciju pretnji i automatizaciju odgovora na incidente. Pruža integraciju sa drugim sigurnosnim proizvodima kompanije Fortinet.

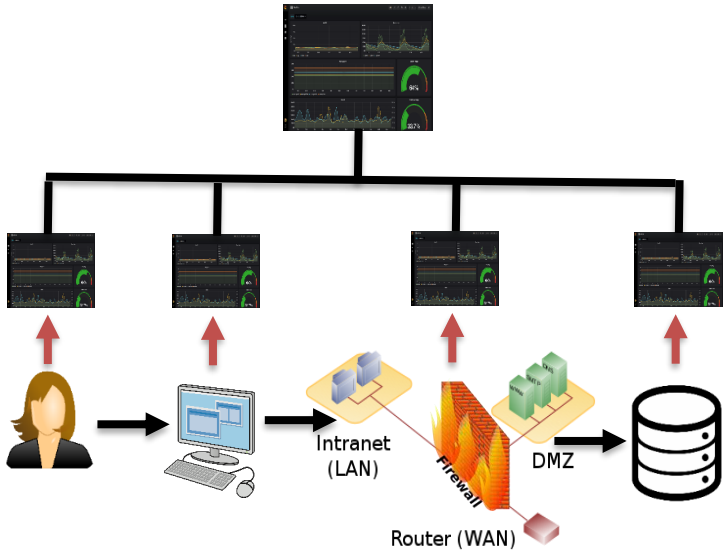
TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

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.

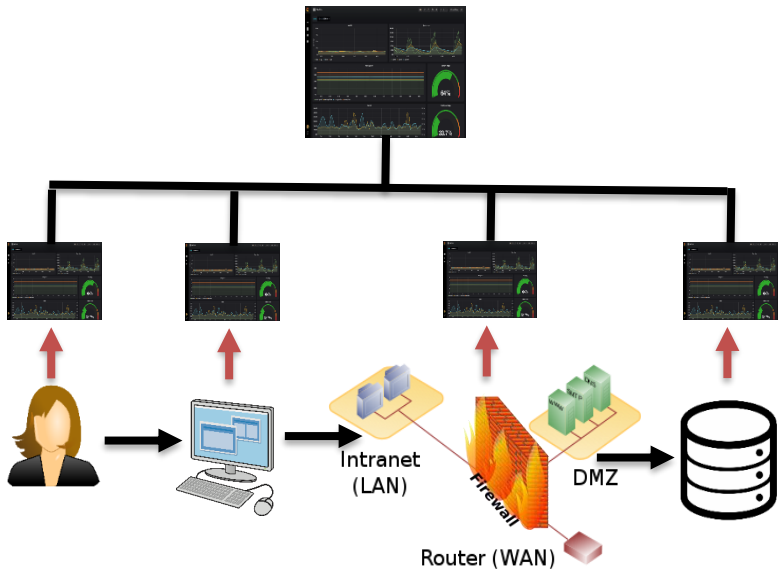


TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

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.



TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

EXTENDED DETECTION AND RESPONSE

Ključne karakteristike EDR tehnologije uključuju:

1.Detekcija pretnji: Praćenje i analiza aktivnosti na endpointima radi identifikacije potencijalno zlonamernih aktivnosti.

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

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

4.Izveštavanje i monitoring: Praćenje sigurnosnih događaja na endpointima i generisanje izveštaja o pretnjama i incidentima.

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

TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

EXTENDED DETECTION AND RESPONSE

CrowdStrike Falcon:

Falcon platforma kompanije CrowdStrike je jedna od najpoznatijih EDR rešenja. Ona pruža naprednu detekciju pretnji, analizu ponašanja i mogućnosti odgovora na incidente na nivou endpointa.

Carbon Black (VMware Carbon Black):

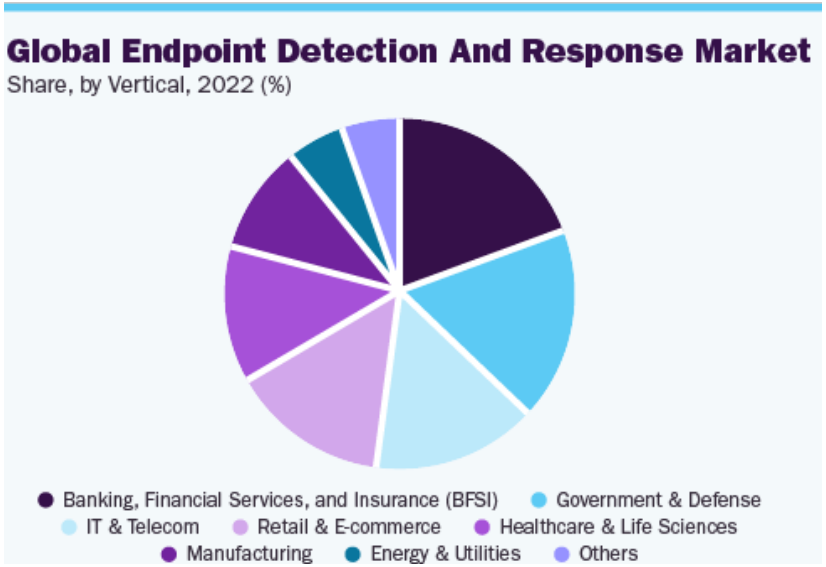
Carbon Black nudi EDR rešenja koja koriste napredne tehnike analize ponašanja kako bi identifikovala pretnje na endpointima. Ova platforma je sada deo VMWare.

Microsoft Defender for Endpoint:

Ovo je integrisano rešenje koje nudi EDR funkcionalnosti u sklopu Microsoft-ovog paketa zaštite, uključujući detekciju pretnji, analizu ponašanja i automatsko reagovanje na incidente.

Symantec Endpoint Detection and Response (EDR):

Symantec nudi EDR rešenje koje kombinuje detekciju pretnji sa analizom ponašanja i mogućnostima odgovora na incidente.



TEHNOLOGIJE ZA DETEKCIJU INCIDENATA

EXTENDED DETECTION AND RESPONSE

Trend Micro Apex One with EDR:

Ova platforma nudi EDR funkcionalnosti u okviru sveobuhvatnog rešenja zaštite krajnjih tačaka koje uključuje antivirusnu zaštitu, detekciju pretnji i zaštitu od ransomware-a.

SentinelOne:

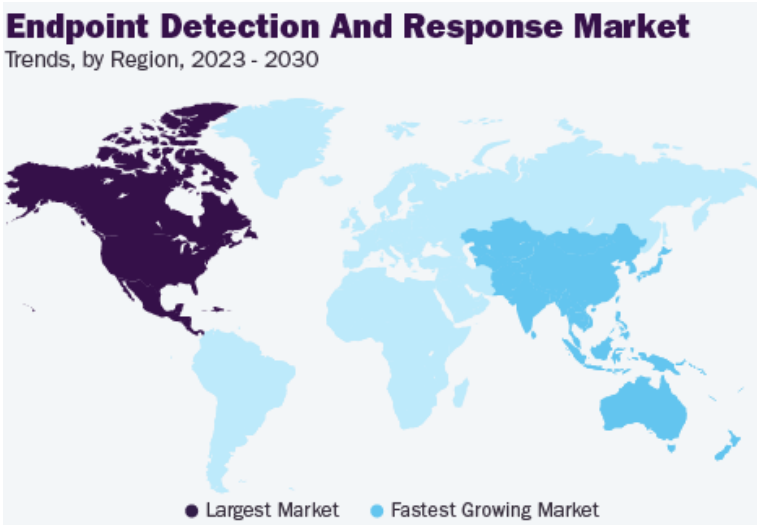
SentinelOne je EDR platforma koja **koristi veštačku inteligenciju i mašinsko učenje za detekciju** i odgovor na pretnje na nivou endpointa.

FireEye Endpoint Security (HX):

FireEye-ov HX proizvod je EDR rešenje koje kombinuje detekciju pretnji sa mogućnostima analize ponašanja i istraživanja incidenata.

Bitdefender GravityZone Ultra with EDR:

Ovo je EDR rešenje koje koristi veštačku inteligenciju i napredne tehnike analize ponašanja za detekciju i sprečavanje kibernetičkih pretnji.



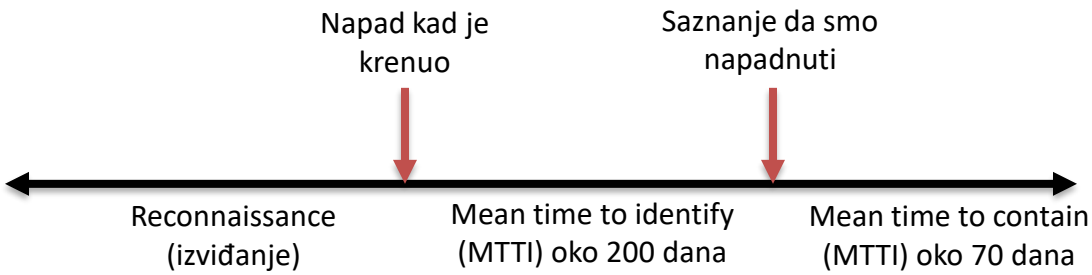
TEHNOLOGIJE ZA DETEKCIJU INCIDENATA
EDR + SIEM

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)



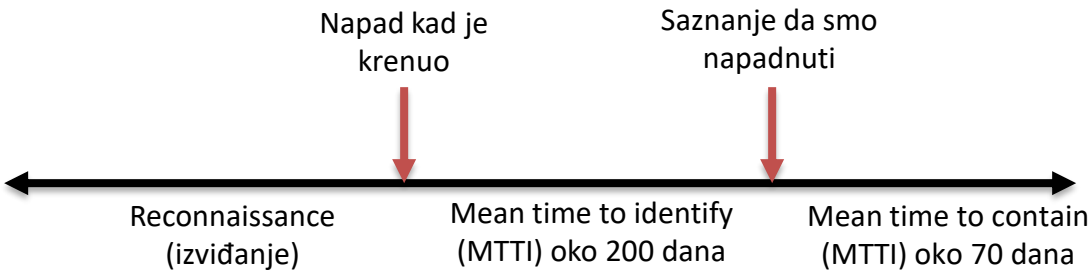
Mean time to identify je prosečno vreme koje protekne od trenutka napada do trenutka kada je kompanija svesna da je napadnuta i iznosi oko 200 dana

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