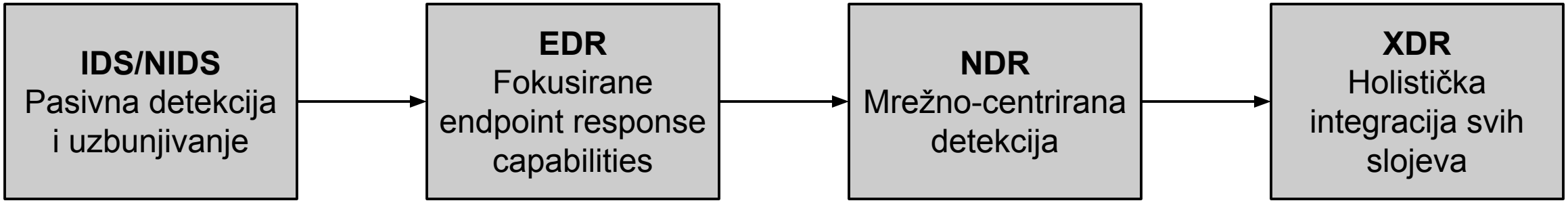
USPOREDBA ALATA ZA NADZOR I INTERVENCIJU NA KRAJNJIM TOČKAMA (ENDPOINT DETECTION AND RESPONSE)

Ante Čavar
Mentor: prof. Stjepan Groš

Pregled predavanja

- Evolucija sigurnosnih tehnologija
- IDS/NIDS
- EDR
- NDR
- XDR
- Usporedbe, preporuke i ključna otkrića
- Zaključak

Evolucija sigurnosnih tehnologija



- Ključno: XDR = NDR + EDR (superset postojećih tehnologija)

IDS/NIDS

- **Ključni alati:**
  - Snort: Najpoznatiji open-source IDS/IPS s pravilima zasnovanim na prepoznavanju uzoraka
  - Suricata: Napredni IDS/IPS s paralelnom obradom paketa i multi-threading podrškom
  - Zeek: Fokus na detaljnu analizu mrežnog prometa umjesto detekcije putem pravila

- Glavna razlika: IDS/NIDS pružaju pasivno nadgledanje, dok DR sustavi omogućavaju aktivno nadgledanje s automatskim odgovorom

Evaluacija performansi

Alat	Točnost detekcije	Performanse	Resursna potrošnja	Prosjek
Suricata	1	1	3	1.67
Zeek	3	2	1	2.00
Snort	2	3	2	2.33

1 = najbolji, 3 = najlošiji

Pobjednik: Suricata - najbolji overall performer s prosječnom ocjenom 1.67

EDR

- Ključne karakteristike
  - Kontinuiran 24/7 nadzor krajnjih točaka
  - Analiza procesa, aplikacija, mrežnih veza i datotečnih operacija
  - "Walled garden" pristup - fokus isključivo na krajnje točke
- Prednosti
  - Visoka granularnost detekcije na razini procesa i datoteka
  - Posebna korisnost za zaštitu udaljenih radnika
  - Mogućnost trenutne izolacije kompromitiranih uređaja
- Ograničenja
  - Ograničena mrežna vidljivost između uređaja
  - Ovisnost o agentima
  - Potencijalna potrošnja resursa

NDR

- Fokus na mrežnu analizu
  - Kontinuiran nadzor mrežnih komunikacija
  - Analiza east-west i north-south prometa
  - Deep packet inspection za detaljnu analizu
- Napredne analitičke metode
  - Strojno učenje za detekciju anomalija
  - Analiza ponašanja za prepoznavanje neobičnih obrazaca
  - Statistička analiza za otkrivanje odstupanja
- Prednosti
  - Vidljivost u cjelokupnu mrežnu infrastrukturu
  - Otkrivanje lateral movement napada
  - Rad bez agenata

XDR

- Sljedeća evolucija sigurnosnih tehnologija
- XDR = "Evoluirana EDR"
- Proširuje fokus s krajnjih točaka na cjelokupno IT okruženje
- Široki spektar nadzora
  - Krajnje točke i mrežni promet
  - Email sustavi i cloud aplikacije
  - Aplikacijski sloj i identity sustavi
- Korelacija podataka
  - Centralizirani pristup analizi sigurnosnih događaja
  - Automatska korelacija između različitih sigurnosnih slojeva
  - Smanjenje false-positive alarma

Tržišni udjeli i pozicioniranje

19.5% **Darktrace** *Dominira IDPS segment kroz AI pristup*	15.5% **CrowdStrike Falcon** *Vodi XDR segment*
13.0% **Wazuh** *Dominantna open-source alternativa*	11.3% **Vectra AI** *AI-pogonjena rješenja*

Analiza ključnih proizvoda

- **Darktrace - Enterprise Immune System**
  - Prednosti: Stabilan rad, informativni alarmi, Antigena za automatiziran odgovor
  - Nedostaci: Visoka cijena, brojni false-positives, slaba integracija
- **CrowdStrike Falcon - Premium endpoint protection**
  - Prednosti: Cloud arhitektura, AI/ML tehnologija, lagan agent
  - Nedostaci: Viša cijena, složenost prilagodbe, strma krivulja učenja
- **Cisco Sourcefire SNORT - Zlatna sredina**
  - Prednosti: 24/7 podrška, dobra integracija, malo false-positives
  - Nedostaci: Performanse se mogu poboljšati, komplicirano postavljanje

Preporuke prema veličini poduzeća

- **Mala poduzeća (1-100 zaposlenika)**
  - Budžet: $5,000-$50,000 godišnje
  - Preporuke: Microsoft Defender XDR, Darktrace, Wazuh
- **Srednja poduzeća (100-1000 zaposlenika)**
  - Budžet: $50,000-$500,000 godišnje
  - Preporuke: Cisco Sourcefire SNORT, SentinelOne, Vectra AI
- **Velika poduzeća (1000+ zaposlenika)**
  - Budžet: $500,000+ godišnje
  - Preporuke: CrowdStrike Falcon, Palo Alto Cortex XDR, Vectra AI

Ključna otkrića

- **Tehnološki trendovi**
  - AI/ML dominacija u svim vodećim rješenjima
  - Cloud-first pristup kao novi standard
  - Konsolidacija alata - preference za integrirane platforme
  - Demokratizacija sigurnosti za manje organizacije
- **Nema "one-size-fits-all" rješenja**
- *Optimalan izbor ovisan je o veličini organizacije, budžetu i tehničkim kapacitetima*
- **Buduće perspektive**
  - Autonomous security s potpuno automatiziranim odgovorom
  - Quantum-resistant security
  - Dublja Zero Trust integracija
  - Proširenje na IoT i edge computing

Zaključak

- **Sigurnosni krajolik kontinuirano evoluira**
- *Od tradicionalnih IDS/NIDS sustava prema sofisticiranim XDR platformama*
- Uspješne organizacije će biti one koje
  - Kombiniraju tehnološku inovaciju s promišljenim strategijskim planiranjem
  - Kontinuirano ulažu u ljudski kapital
  - Prilagođavaju odabir tehnologija specifičnim organizacijskim potrebama
  - Fokusiraju se na proper implementation i ongoing optimization

Hvala!