Tjedan 10.3. - 14.3.

#seminar2

EDR

EDR (engl. **E**ndpoint **D**etection and **R**esponse) je "tehnologija" koja konstantno nadzire krajnje točke (endpoints) tj. laptope, mobitele i ostalu računalnu opremu sa mogućnosti povezivanja na unutrašnji sustav neke organizacije.

- prati samo krajnje točke (walled garden)
- ponaša se prema svakom uređaju kao vektoru napada
- najčešće koriste ogromne organizacije
- najkorisniji za rad od doma
- pruža administratorima vidljivost i pristup svim računalima sa potrebnom programskom potporom

https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response

Primjeri:

- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- SentinelOne
- Carbon Black (VMware)
- Cybereason

XDR

XDR (engl. **E**xtended **D**etection and **R**esponse) je tehnologija koja kombinira više elemenata IT okoline neke organizacije poput maila, mreža, aplikacija kao i samu analizu krajnjih točki. Još se zato naziva evoluirana EDR.

- prati mail, mrežu, aplikacije...
- manje false-positive alarma (naspram EDR)

- analizira "veći prostor" (naspram EDR)
- bolja efikasnost i ranije primjećivanje

https://corelight.com/resources/glossary/xdr-extended-detection-and-response

https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR

https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/extended-detection-and-response-xdr/

Primjeri:

- Palo Alto Networks Cortex XDR
- Trend Micro Vision One
- Microsoft Defender XDR (formerly Microsoft 365 Defender)
- CrowdStrike XDR
- SentinelOne Singularity XDR
- Wazuh

NDR

NDR (engl. **N**etwork **D**etection and **R**esponse) je tehnologija slična EDR samo radi na mreži a ne na krajnjim točkama.

- sprema mrežni promet sa vatrozida, rutera i switcheva
- koristi strojno učenje, analizu ponašanja i *signature/fingerprint* analizu

https://www.fortinet.com/resources/cyberglossary/what-is-ndr

https://www.cisco.com/c/en/us/products/security/what-is-network-detection-response.html

Primjeri:

- Darktrace
- Vectra AI
- Cisco Stealthwatch
- ExtraHop Reveal(x)
- FireEye Network Security (now part of Trellix)

IDS/NIDS

IDS (engl. *Intrusion Detection System*) je sistem za skeniranje sustava i detekciju upada.

NIDS (engl. *Network Intrusion Detection System*) je sistem za skeniranje mreže sustava i detekciju upada.

Primjeri:

- Snort
- Suricata
- Zeek

$$(NDR|EDR) \subset XDR$$

$$NIDS \subset IDS$$

$$IDS \subset XDR$$

Najbitnije razlike:

- IDS-ovi samo traže upade dok *Detection and Response* (nadalje DR) sustavi mogu imati konfigurirane automatske radnje prilikom detekcije upada što im je ujedno i jedina razlika
- DR-ovi se tretiraju kao skuplji i bolji proizvod a od njih najtraženiji su XDR-ovi