# Endpoint Detection & Response

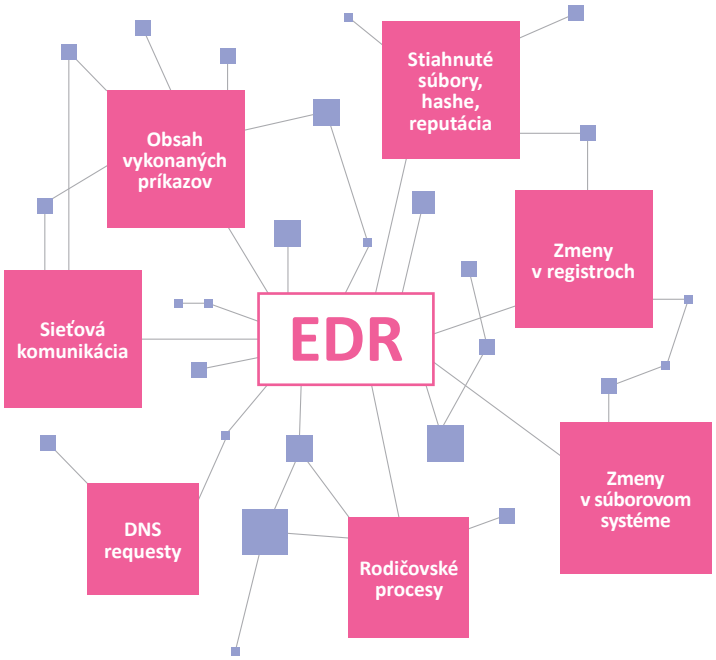

AEC

Endpoint Detection and Response (EDR) produkty slúžia k ochrane koncových staníc pred škodlivým kódom a prienikom útočníka. Od bežných antivírusových produktov sa líšia logovaním dôležitých aktivít na koncových staniciach a širokými možnosťami pri riešení incidentu.

www.aec.sk

## Zber informácií

Riešenie EDR umožňuje zbierať informácie o aktivitách na koncových staniciach a vďaka tomu umožňuje efektívne vyhodnotiť bezpečnostný incident. Nie je potreba integrovať žiadne zdroje logov do EDR nástroja, všetko zaistí agent na koncovej stanici, jeho inštalácia zaberie iba desiatky sekúnd a je možné vykonať ju centrálne.



## Prečo zvoliť EDR od AEC?

### 1 Vykonáme analýzu incidentu

- Ako sa útočník dostal do systému
- Aké boli aktivity útočníka
- Ako zabrániť podobnému incidentu v budúcnosti

### 2 Reagujeme ihneď

- Príjazd bezpečnostného tímu do 3 hodín
- Sledovanie útočníka a jeho zablokovanie real-time
- Stiahnutie podozrivých súborov k analýze

### 3 Pomôžeme zastaviť útok

- Vynútené ukončenie škodlivého procesu
- Odrezanie stanice od siete
- Vymazanie pozostatkov útočníka

### 4 Kontinuálny dohľad

- Režim 24/7 alebo 8/5
- Bezpečnostný analytik na telefóne
- Pravidelný reporting menej závažných aktivít

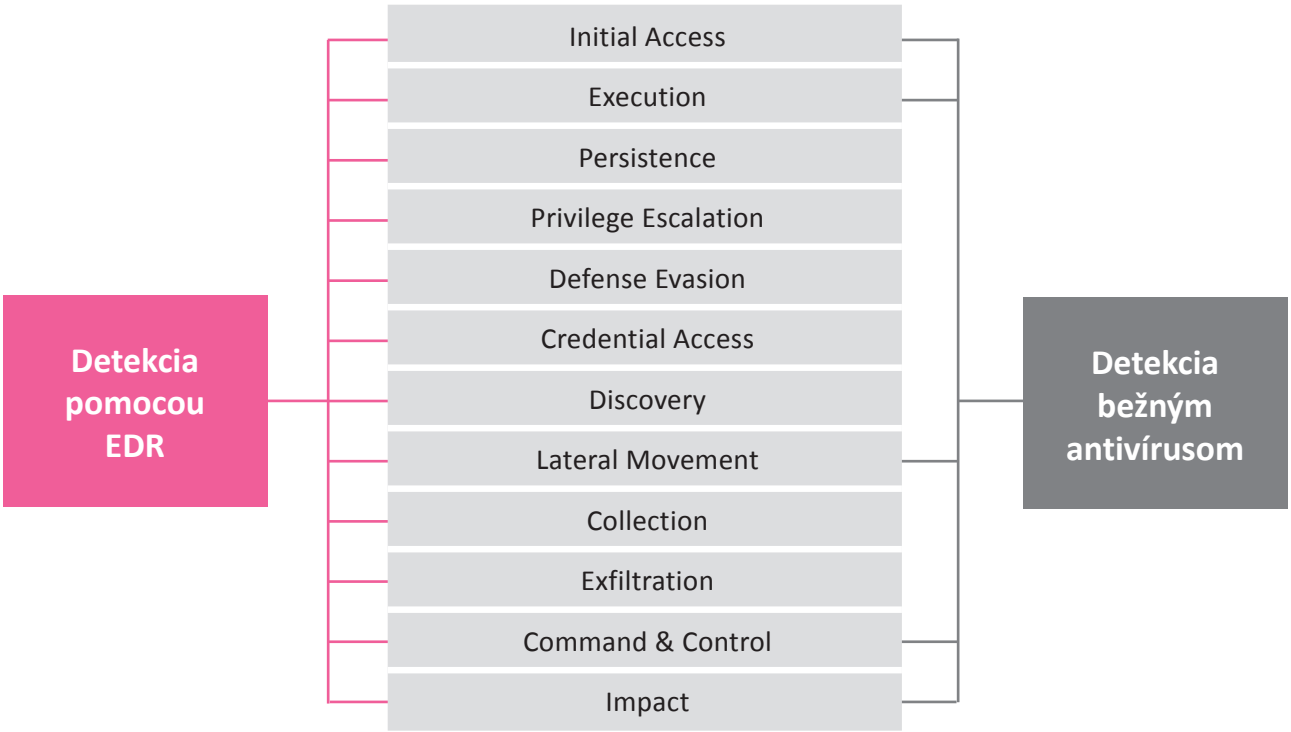
## Keď interné sily nestačia

Vyhodnotiť správne všetky bezpečnostné udalosti môže byť časovo aj kapacitne náročné. Preto ponúkame taktiež služby nášho bezpečnostného operačného centra Cyber Defense Center. Naši analytici vyhodnocujú udalosti a v prípade problémov môžu okamžite reagovať.

## Čo má EDR naviac oproti AV?

- Zber informácií o spustených procesoch
- Pokrytie celého spektra MITRE ATT&CK taktík využívaných pri útoku
- Tvorba vlastných YARA pravidiel
- Vynútenie ukončenia procesu a zablokovanie sieťovej komunikácie

## MITRE ATT&CK taktiky




AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283