Endpoint Detection & Response

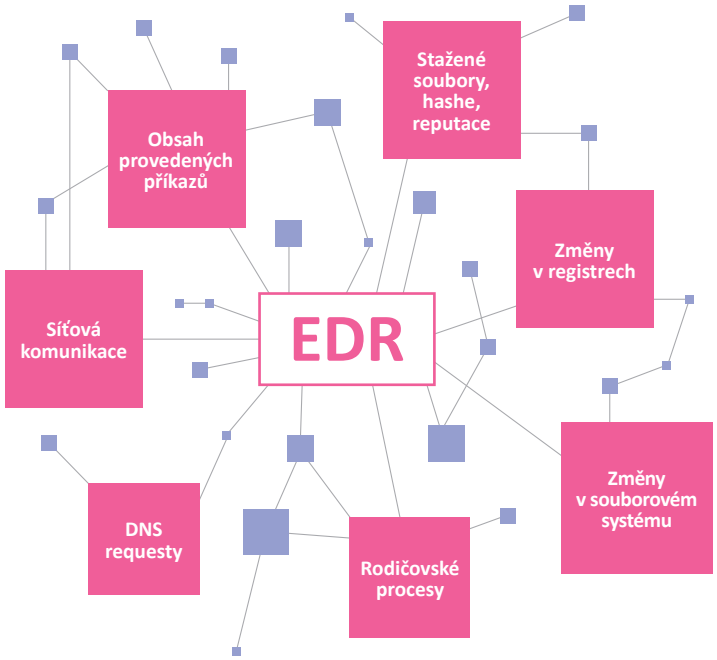
AEC

Endpoint Detection and Response (EDR) produkty slouží k ochraně koncových stanic před škodlivým kódem a průnikem útočníka. Od běžných antivirových produktů se liší logováním důležitých aktivit na koncové stanici a širokými možnostmi při řešení incidentu.

www.aec.cz

Sběr informací

Řešení EDR umožňuje sbírat informace o aktivitách na koncové stanici a díky tomu umožnit efektivní vyhodnocení bezpečnostního incidentu. Není potřeba integrovat žádné zdroje logů do EDR nástroje, vše zajistí agent na koncové stanici, jehož instalace zabere pouze desítky sekund a je možné ji provést centrálně.



Proč zvolit EDR od AEC?

1

Provedeme analýzu incidentu

- Jak se útočník dostal do systému
- Jaké byly útočníkovy aktivity
- Jak zabránit podobnému incidentu v budoucnosti

2

Reagujeme okamžitě

- Dojezd bezpečnostního týmu do 3 hodin
- Sledování útočníka a jeho zablokování real-time
- Stažení podezřelých souborů k analýze

3

Pomůžeme zastavit útok

- Vynucené ukončení škodlivého procesu
- Odříznutí stanice od sítě
- Vymazání pozůstatků útočníka

4

Kontinuální dohled

- Režim 24/7 nebo 8/5
- Bezpečnostní analytik na telefonu
- Pravidelný reporting méně závažných aktivit

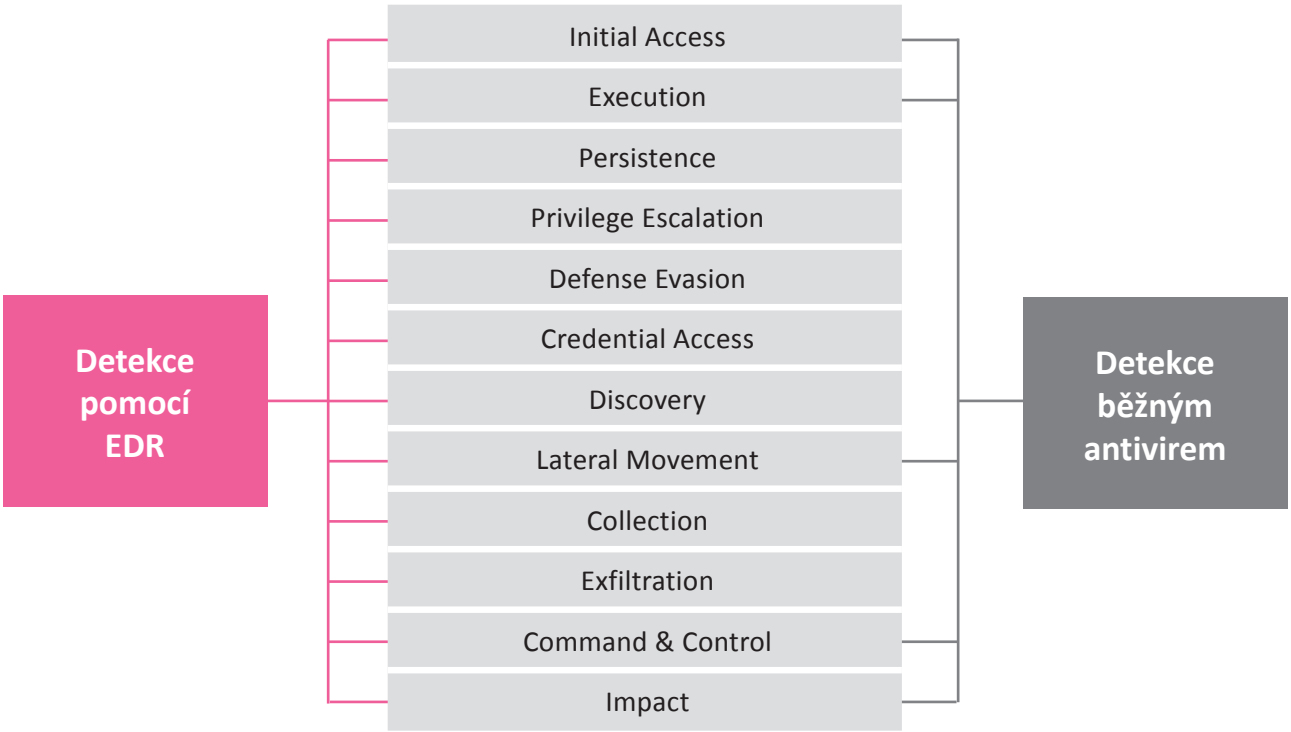
Když interní síly nestačí

Vyhodnotit správně všechny bezpečnostní události může být časově i kapacitně náročné. Proto nabízíme také služby našeho bezpečnostního operačního centra Cyber Defense Center. Naši analytici vyhodnocují události a v případě problémů mohou okamžitě reagovat.

Co má EDR navíc oproti AV?

- Sběr informací o běžících procesech
- Pokrytí celého spektra MITRE ATT&CK taktik využívaných při útoku
- Tvorba vlastních YARA pravidel
- Vynucení ukončení procesu a zablokování síťové komunikace

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