ARICOMA

EDR/XDR

Za časů obávaných virů, mocných hackerů a zdokonalující se generativní AI, neklidem otřesení bezpečnostní analytici stvořili hrdiny, jejichž úkolem je vzdorovat těmto obávaným nepřátelům. Viditelnost, škálovatelnost a AI se vtělily do mocných nástrojů EDR a XDR s úkolem zvrátit průběh nerovného boje a udělat tak kyberprostor bezpečnější.

Přístup, kdy byla zařízení chráněna firmou vytvořeným bezpečnostním perimetrem, již v éře Home Office a cloudových technologií nedostačuje. Význam síťového perimetru se vytrácí a přichází **čas na ochranu jednotlivých zařízení**.

Endpoint Detection and Response (EDR) a Extended Detection and Response (XDR) systémy představují inovaci v kybernetické obraně, posunující bezpečnostní paradigma od statických detekčních modelů k dynamickému sledování a reakci.

Vzhledem k tomu, že vývoj umělé inteligence umožňuje rychlé generování malwaru a C&C. Díky tomu statické detekční metody založené na indikátorech kompromitace (IOC) ztrácejí svoji účinnost.

Mají antivirová řešení v současné době smysl?

Vzniká tedy otázka, zda tradiční antivirové programy mají stále své místo v současném bezpečnostním ekosystému. EDR přineslo revoluci v ochraně koncových stanic a může se zdát, že dny klasických antivirů jsou sečteny. Proti sofistikovaným hrozbám dneška je zapotřebí robustnější obrany!

Rozšíření detekčních schopností EDR

Pro zvýšení účinnosti EDR je vhodné jej integrovat s daty z aplikací a technologií třetích stran. Toto rozšíření umožňuje nejenom sofistikovanější vyhodnocení dat pomocí AI, ale i implementaci automatických odpovědí založených na definovaných scénářích. Takový přístup zvyšuje celkovou odolnost systémů proti kybernetickým hrozbám. Tímto rozšířením se z EDR stává XDR, ale aby to nebylo moc jednoduché je více možností, jak XDR dosáhnout.

Definice XDR

V současné době neexistuje na trhu jednotný způsob, jak lze XDR popsat. I přestože přístupy jsou rozdílné tak lze XDR definovat jako technologii, která v sobě kombinuje data z koncových stanic (EDR) a data z ostatních bezpečnostních technologií a systémů, které jsou v současné době používány (Antispam, DLP, apod.).

XDR tedy může být samostatnou technologií, anebo XDR může být označení pro stav, kdy je využíváno více technologií, které vedou k XDR. Součástí tohoto mixu určitě musí být i SIEM, ale jak už název napovídá SIEM není XDR.

Rozdíl mezi XDR a SIEM

XDR se zaměřuje především na detekci a reakci, přičemž využívá data z různých zdrojů v síti, včetně koncových bodů, cloudových služeb a e-mailových systémů. K detekci hrozeb a automatizaci reakcí napříč těmito různými vektory využívá pokročilou analytiku, umělou inteligenci (AI) a strojové učení (ML). V takovém případě nemusí mít bezpečnostní analytik všechny informace proč došlo k detekovaní vybrané události, nicméně tento přístup vykazuje poměrně malé False Positive Rate (FPR).

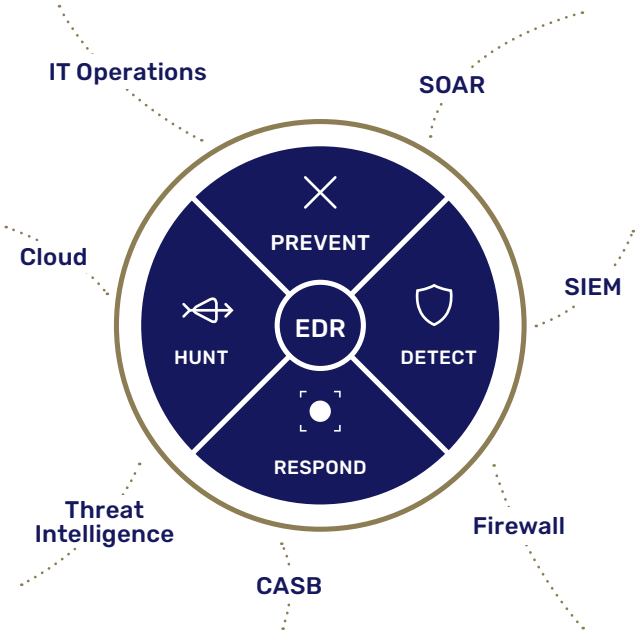
SIEM se zaměřuje na správu protokolů, korelaci událostí a upozorňování v reálném čase. Shromažďuje a agreguje data z různých zdrojů v prostředí IT, jako jsou síťová zařízení, systémy a aplikace, s cílem identifikovat anomální chování a potenciální bezpečnostní incidenty. Přičemž k detekci jednotlivých událostí, se používají statická korelační pravidla. Díky tomu, má bezpečnostní analytik všechny informace, proč došlo k detekovaní vybrané události, ale tato pravidla manuálně udržovat a rozvíjet. Takto vytvořená a upravená pravidla mají vysokou míru FPR.

Co EDR přinese

- EDR zajišťuje komplexní detekci hrozeb, analýzu incidentů a okamžitou reakci na útoky, jejichž cílem je kompromitace koncové stanice.
- Poskytuje hluboký vhled do systémových procesů, což je nezbytné pro proaktivní hledání a odhalování skrytých hrozeb, tzv. Threat Hunting.

Co XDR přinese

- XDR zajišťuje komplexní detekci hrozeb, analýzu incidentů a okamžitou reakci na útoky v celé infrastruktuře.
- Oproti EDR poskytuje detailní vhled do napojených technologií v rámci vaší organizace.



Zastupujeme tyto společnosti

SentinelOne · CROWDSTRIKE · ESET · CHECK POINT · IBM Security