XDR (Extended Detection and Response)

XDR odstraňuje tzv. „bezpečnostní sila“. V běžné firmě má e-mailový filtr, firewall a antivirus vlastní konzoli. Útočník se může pohybovat mezi těmito systémy nenápadně. XDR všechna tato data slije do jednoho „jezera“ (Data Lake), kde je analyzuje pomocí umělé inteligence.

1. Hlavní rozdíly: EDR vs. XDR

XDR není náhradou za EDR, ale jeho evolucí.

Vlastnost	EDR	XDR
Rozsah dat	Pouze koncová zařízení (PC, servery)	PC + síť + cloud + e-mail + identity
Kontext	Vidí, co se stalo na jednom stroji	Vidí, jak útok začal e-mailem a pokračoval v síti
Detekce	Zaměřeno na procesy a soubory	Zaměřeno na komplexní vzorce chování
Reakce	Izolace počítače	Zablokování uživatele v Cloudu, změna pravidel firewallu

2. Jak XDR řeší "únavu z alarmů" (Alert Fatigue)

Bezpečnostní analytici jsou často zaplaveni tisíci varováními denně. XDR používá **korelaci událostí**:

- **Tradiční systém:** Vygeneruje 3 různé alarmy (1. podezřelý e-mail, 2. divné přihlášení, 3. neznámý proces na PC).
- **XDR:** Spojí tyto 3 události do jednoho **Incidentu**. Analytik vidí, že jde o jeden útok, a nemusí řešit tři izolované problémy.

3. Klíčové komponenty XDR

- **Data Lake (Datové jezero):** Centrální úložiště pro všechny protokoly (logy) z celé firmy.
- **Analytický engine:** Využívá strojové učení k odhalování „pomalých a tichých“ útoků, které by člověk přehlédl.
- **Automatizace (SOAR):** Schopnost systému automaticky provést protiakci (např. pokud je detekován únik dat, XDR okamžitě zablokuje dotyčný uživatelský účet v Microsoft 365 i v lokální síti).

4. Typy XDR řešení

- **Nativní XDR:** Všechny komponenty (antivirus, firewall, cloud) jsou od jednoho výrobce. Výhodou je dokonalá integrace.
- **Otevřené (Open) XDR:** Dokáže spolupracovat s nástroji od různých výrobců. Výhodou je, že firma nemusí měnit svůj stávající hardware.

5. Přínos pro moderní IT

V době, kdy zaměstnanci pracují z domova a využívají cloudové služby, už klasický firewall na hranici firmy nestačí. XDR poskytuje ochranu tam, kde se zrovna nachází data a uživatelé, bez ohledu na to, zda jsou v kanceláři nebo v kavárně.

> **Zajímavost:** XDR je považováno za klíčový prvek architektury **Zero Trust** (nikomu nevěř). V tomto modelu se neustále prověřuje identita a chování každého uživatele i zařízení, a právě XDR k tomu dodává potřebná data v reálném čase.

Zpět na Bezpečnost