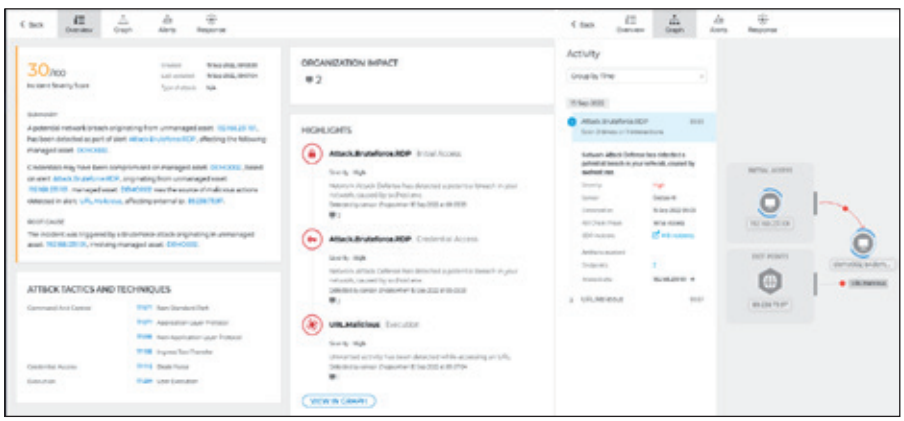
Jaké výhody přináší XDR oproti EDR?

EDR, nebo XDR? Otázka, kterou si položilo mnoho bezpečnostních pracovníků v organizacích po celém světě.

Vývoj bezpečnostních technologií v posledních letech zařadil vyšší rychlostní stupeň a není vždy jasné, která platforma bude mít pro organizaci nejvyšší přínos v poměru cena/výkon. K zodpovězení mnoha dotazů ohledně bezpečnosti pomohou analýzy rizik, ale na otázku, zda pořídit EDR, nebo XDR řešení, nebývá zcela jasná, jednoduchá odpověď, přitom XDR řešení bývají výrazně dražší než EDR. Vyplatí se organizaci si připlatit? Pokusím se stručně ukázat, jaké jsou hlavní přínosy XDR řešení na příkladu jednoho útoku očima EDR a z hlediska XDR…

Obr. 1: ukázka detekce probíhajícího útoku v EDR incidentu – úspěšný bruteforce útok na RDP



Obr. 2: ukázka detekce probíhajícího útoku v XDR incidentu – na první pohled jasné, odkud útok přišel a jaký byl celkový zásah

EDR

EDR (Endpoint Detection and Response) řešení sbírají informace o běhu systému, aplikací a síťovém provozu na každém koncovém bodě. Tyto údaje zpracovává v reálném čase – prakticky se v každém momentě rozhoduje, zda dění na počítači nenaznačuje, že na daném přístroji právě probíhá kybernetický útok. Ve chvíli, kdy je takový útok odhalen, vytvoří EDR řešení ve svém ovládacím rozhraní bezpečnostní incident, ve kterém definuje, které chování koncového bodu je podezřelé a naznačuje, že došlo k prolomení bezpečnosti. Pokročilá EDR řešení, jako je Bitdefender GravityZone Business Security Enterprise, automaticky otagují každý krok útoku MITRE ATT & CK (https://attack.mitre.org/) taktikami a technikami – na první pohled tedy bezpečnostní pracovníci vidí, čeho se snažil útočník v rámci útoku docílit a jakým způsobem toho dosáhl. To umožňuje rychlou reakci a urychluje sběr dat pro forenzní analýzu útoku. Kromě toho jsou umožněny rychlé reakce, jako je např. odpojení napadeného koncového bodu ze sítě. EDR systémy jsou velmi mocné a bezpečnostním týmům umožní vhled do průběhu útoků, jaký dříve neměli, ale co když analýza napadení pouze v kontextu jednoho koncového bodu nestačí?

XDR

Odpověď na tuto otázku přináší právě XDR (eXtended Detection and Response) řešení. Rozšířeny jsou o další typy zdrojů dat, jako jsou síťové sondy, sondy do systémů ověřujících identitu uživatelů (např. Active Directory), sondy do cloudových služeb, sondy do e-mailových serverů apod. Dále jsou rozšířeny o množství akcí, které umožňují např. blokování uživatelských účtů. Zdaleka nejvyšší přínos je však v tom, že detekce a analýza útoků se děje v kontextu celé organizace, a ne pouze jednoho koncového bodu. Bezpečnostní incidenty, které XDR systémy vytvářejí, tak ukazují průběh útoku napříč celou organizací. Bitdefender XDR sumarizuje, jaké kroky útoku měly největší zásah, a usnadňuje tak bezpečnostnímu pracovníkovi rozhodovací proces ohledně určení priority akcí, které budou v reakci na odhalený probíhající útok uskutečněny.