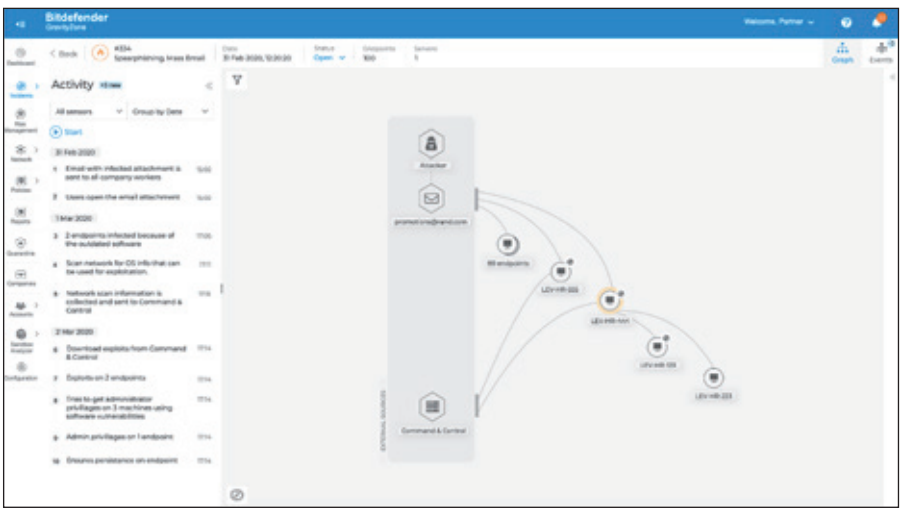
Jak Bitdefender XDR šetří čas při vyšetřování bezpečnostních incidentů?

Bitdefender letos v dubnu vydal své XDR řešení v rámci bezpečnostní platformy GravityZone. Bitdefender tak rozšířil své úspěšné EDR řešení (zdrojem dat jsou koncové body) o další typy senzorů.



Ukázka reálného bezpečnostního incidentu v Bitdefender XDR (anonymizováno) – na první pohled je vyznačeno, že útok začal příchozími e-mailovými zprávami. U dvou uživatelů na dvou koncových bodech došlo k nákaze díky zastaralé zranitelné verzi aplikace, a tyto stanice poslaly útočníkovi informace o síti a zjištěné aplikační výbavě dalších koncových bodů na jeho C2 server. Zpět obdržely útočný kód, díky kterému si zabezpečil eskalaci privilegií na administrátora, a zajistil perzistenci na tomto systému.

Nově je možné řešení Bitdefender GravityZone Business Security Enterprise, které obsahuje plnohodnotné automatizované EPP a XEDR, rozšířit o následující senzory, a získat tak automatizované XDR:

- Active Directory – audit přístupů a administrátorských akcí
- Azure Active Directory – audit přístupů a administrátorských akcí
- Office 365 (nově Microsoft 365) – e-mailový provoz a audit přístupů
- Amazon Web Services – audit přístupů a administrátorských akcí
- síťové sondy – virtuální zařízení do VMwaru či Hyper-V, které analyzuje kopii veškerého síťového provozu v organizaci

Tyto další zdroje dat zvyšují kvalitu informací podávaných správcům bezpečnosti v organizaci o uskutečňujících se/uskutečněných bezpečnostních incidentech (kybernetických útocích), a zároveň rozšiřují detekční schopnosti celé bezpečnostní platformy GravityZone.

Proč je XDR lepší než EDR či XEDR? EDR systém ukazuje analýzu průběhu útoku v rámci jednoho koncového bodu, XEDR ukazuje průběh a analýzu útoku napříč všemi koncovými body, XDR ukazuje průběh útoku napříč celou sítí (síťová sonda) včetně vybraných cloudových služeb (AAD, O365, AWS). Též díky těmto sondám umožňuje více reakcí – např. zablokování/smazání nově vzniklého uživatelského účtu. Tyto sondy též pomáhají snižovat počet falešně pozitivních detekcí – čím více a čím kvalitnější data dostává Gravityzone XDR, tím přesnější je automatická analýza, kterou provádí umělá inteligence, a tím bohatší data může bezpečnostním týmům v organizaci poskytnout.

V přiložených ukázkách můžete vidět, že místo přehršle logů a nezpracovaných informací vytváří Bitdefender XDR pomocí automatické analýzy ucelený přehled průběhu celého útoku a jeho jednotlivé kroky značí technikami a taktikami podle matice MITRE ATT & CK® (*https://attack.mitre.org/*). To vše v reálném čase. Dodává tak správcům bezpečnosti v organizaci důležité informace, na základě kterých mohou okamžitě jednat.

Na první pohled je vidět, z jakého vektoru útok přišel, kolik a které typy koncových bodů byly zasaženy, jaké byly postupné kroky útočníka, a v přehledu jsou vidět nejdůležitější kroky útočníka (např. původní přístup byl pomocí phishingového e-mailu, který otevřel uživatel XY, pak útočník provedl průzkum sítě, aby si vybral cíl dalšího kroku svého útoku, provedení laterálního pohybu apod.). Bezpečnostní incident je u právě probíhajícího útoku aktualizován v reálném čase a doplňován o každý další krok, který útočník provádí. Bezpečnostní tým může pochopitelně útočníka „odstřihnout" – zrušit přístup do sítě stroji, jenž k útoku zneužívá, zablokovat uživatelský účet, který zneužívá, apod., a to přímo z ovládací konzole Bitdefender GravityZone – tyto akce jsou bezpečnostnímu týmu přímo nabídnuty a na jedno kliknutí mohou být provedeny.

Bitdefender XDR též rozšiřuje možnosti vyšetřování průlomů (tzn. threat hunting), a to díky možnosti stažení balíčku forenzních dat z jakéhokoli koncového bodu, nebo možnosti vyvolat si výchozí CLI (textové rozhraní – např. Powershell, bash, zsh) na jakékoli stanici/serveru (Windows workstation i Windows Server, Linux a MacOS) – vše z jednoho místa, bez potřeby řešení třetích stran. Veškerá aktivita během takovéhoto spojení je logována a log je uložen pro účely auditu.

V přiložených ukázkách můžete vidět, že místo přehršle logů a nezpracovaných informací vytváří Bitdefender XDR pomocí automatické analýzy ucelený přehled průběhu celého útoku a jeho jednotlivé kroky značí technikami a taktikami podle matice MITRE ATT & CK® (*https://attack.mitre.org/*). To vše v reálném čase. Dodává tak správcům bezpečnosti v organizaci důležité informace, na základě kterých mohou okamžitě jednat.