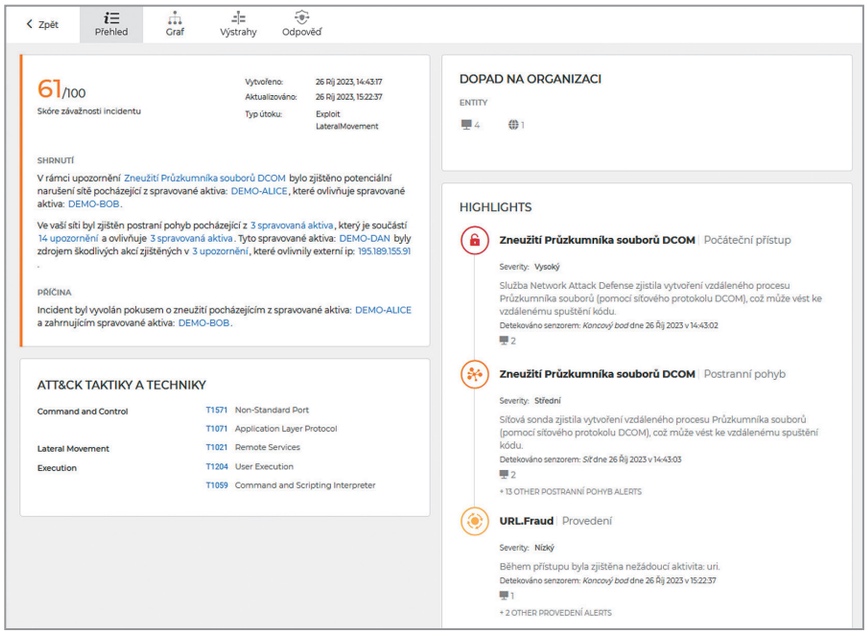
Bitdefender XDR vám pomůže zkrátit čas potřebný k účinnému zastavení kybernetického útoku

Bitdefender loni v dubnu vydal své XDR řešení v rámci bezpečnostní platformy GravityZone a od té doby ho neustále vylepšuje.



Nyní je možné EDR rozšířit o velké množství druhů senzorů – Active Directory, Azure Active Directory, Microsoft 365, Google Workspace, Microsoft Intune, Google Cloud, Azure Cloud, Amazon Web Services, síťová sonda – a byly značně rozšířeny schopnosti řešení pro tzv. threat hunting (hledání hrozeb) pomocí funkce Live Search s více než 300 předdefinovanými dotazy (např. vyhledání všech strojů, které jsou zranitelné na log4j, všechny stroje, jež mají nějaké otevřené porty, všechny stroje, na kterých běží nějaká aplikace, apod.). Live Search využívá jazyk OSQuery, jenž je podobný SQL jazyku a stal se v oboru standardem. Rozšířeny byly též možnosti přidání vlastních detekčních pravidel, kdy je nyní možnost vytvářet vlastní detekční pravidla s využitím jazyka YARA, který je taktéž v oboru standardem. Mnoho bezpečnostních výzkumníků v článcích popisujících hrozbu, již zkoumali, uvádí YARA pravidla pro detekci zkoumané hrozby, takže pak stačí tato pravidla pouze zkopírovat, a pokud by se hrozba ve vaší síti vyskytovala, bude vytvořen bezpečnostní incident a můžete na hrozbu reagovat.

Jaké výhody přináší XDR oproti EDR? EDR systém ukazuje analýzu průběhu útoku v rámci jednoho koncového bodu, XDR systém ale ukazuje průběh útoku napříč celým prostředím organizace, včetně využitých cloudových služeb a díky tomu umožňuje okamžitou reakci bezpečnostního týmu. Kromě toho prezentuje celkový zásah organizace včetně toho, které uživatelské účty byly v rámci útoku prolomeny, jaké byly nově vytvořeny, které všechny stroje byly napadeny, jaké soubory byly odeslány na server útočníka atd. To vše v reálném čase.

V přiložených ukázkách můžete vidět, že místo přehršle logů a nezpracovaných informací vytváří Bitdefender XDR pomocí automatické analýzy ucelený přehled průběhu celého útoku, jeho rychlé shrnutí a identifikuje původce. Jednotlivé kroky útoku taguje technikami a taktikami podle matice MITRE ATT & CK® (*https://attack.mitre.org/*). Dodává tak správcům bezpečnosti v organizaci okamžitý přehled o rozsahu útoku a veškerých aktivitách útočníka.

Na první pohled je vidět, z jakého vektoru útok přišel, kolik a které koncové body byly zasaženy, jaké byly postupné kroky útočníka, a adresa serveru útočníka, jenž využil pro exfiltraci dat. V přehledu jsou vidět nejdůležitější kroky útočníka (původní přístup byl ze stanice demo-alice, pak došlo k laterálnímu pohybu skrz stroje demo-bob, demo-charlie až na stroj demo-dan a ze stroje demo-dan byla provedena exfiltrace dat na IP adresu 195.189.155.91). Bezpečnostní incident je u právě probíhajícího útoku aktualizován v reálném čase a doplňován o každý další krok, který útočník dělá. Bezpečnostní tým může pochopitelně útočníka „odstřihnout" – zablokovat přístup do sítě strojům, které k útoku zneužívá, a připojit se na příkazový řádek těchto strojů (powershell, bash, zshell), zablokovat uživatelský účet, jenž 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 nabízí představení a bezplatné vyzkoušení Bitdefender GravityZone Business Security Enterprise včetně všech XDR sond i pro vaši organizaci. Se žádostí o provedení PoC se obracejte na *info@bitdef.cz*.