Bitdefender
BUILT FOR RESILIENCE

GravityZone XDR

Extended Detection and Response

Četnost kybernetických útoků a jejich sofistikovanost exponenciálně vzrostly. Celé podniky byly vyřazeny z provozu pouhým kliknutím na adresu URL v e-mailu. Pokročilé trvalé hrozby mohou zůstat neodhaleny celé měsíce, zatímco z podniků odčerpávají data, podstrkují ransomware a mažou soubory z kritických systémů. K této situaci se přidal i nástup práce z domova a hybridních pracovních modelů, které přinesly nové vektory útoku, jež mohou kybernetičtí zločinci využívat. Přestože se technologie prevence kybernetické kriminality zdokonalily, bezpečnostní experti uznávají, že 100% prevence je nedosažitelná, protože útočníci se ve svých taktikách, technikách a postupech neustále zdokonalují. Vzhledem k této skutečnosti jsou informace nejlepším nástrojem, který mohou bezpečnostní týmy využít ke zkrácení doby pro jejich detekování, a v konečném důsledku ke snížení rizika škod a zvýšení kybernetické odolnosti.

Potřeba shromažďovat a analyzovat různorodé bezpečnostní informace vedla k přechodu od technologií EDR (endpoint detection and response) k technologiím XDR (extended detection and response). Technologie XDR je navržena tak, aby rozšířila možnosti EDR tím, že umožňuje přijímat informace z více zdrojů dat, poskytuje jasnější obraz o jednotlivých krocích útoku, a umožňuje identifikovat účinnější způsoby reakce.

Zvýšená komplexnost kybernetických útoků, které se odehrávají ve více segmentech, vedla k vývoji technologie XDR. Účinná technologie XDR musí mít následující schopnosti:

- Shromažďování dat ze zdrojů, které mohou při kybernetickém útoku fungovat jako místa kompromitace.
- Pokročilé strojové učení a umělá inteligence, které analyzují data a odhalují relevantní informace.
- Eliminace nadbytečného šumu při vyšetřování útoku zabraňuje únavě z falešně pozitivních výstrah.
- Poskytuje bezpečnostním týmům nástroje pro přijetí okamžitých opatření.

Jak XDR rozšiřuje detekci a reakci za hranice koncového bodu

GravityZone XDR kombinuje oceňované technologie detekce a prevence Bitdefender s výkonnými senzory, pokrývajícími systémy, produktivní aplikace, cloudové pracovní zátěže, identity a sítě. Díky GravityZone XDR mají bezpečnostní týmy rozšířený přehled o celém životním cyklu útoku - od počátečního bodu napadení, přes laterální pohyb a mnoho dalšího. GravityZone XDR poskytuje podrobnou analýzu kořenových příčin a rozšířené zobrazení hrozeb, které přesahují hranice koncového bodu.

Přehledně

GravityZone XDR analyzuje a detekuje útoky napříč infrastrukturou a aplikacemi organizace s pomocí přesnější detekce a rychlá reakce. GravityZone XDR pokrývá systémy, produktivní aplikace, cloudové pracovní zátěže, identity a sítě, a pomáhá bezpečnostním týmům zaměřit se na klíčové oblasti, které jsou cílem kybernetických útoků. Poskytuje analytiku a bohatý bezpečnostní kontext pro korelaci různorodých výstrah, rychlé třídění incidentů a omezení útoků prostřednictvím automatizované a řízené reakce. To vše bez zatěžování bezpečnostních týmů zbytečnými výstrahami - dostupné z jednotné, intuitivní konzole pro správu.

Hlavní výhody

- Detekuje kybernetické útoky napříč systémy, produktivními aplikacemi, cloudovými pracovními úlohami, identitami a sítěmi.
- Poskytuje analýzu hlavních příčin, kterou mohou bezpečnostní týmy následně přezkoumat
- Vizualizuje kompletní řetězec útoku ve snadno stravitelném formátu, aby bylo možné identifikovat slabá místa v rámci bezpečnostního řetězce
- Rychle provádí odvetná opatření - odstraňuje škodlivé e-maily, izoluje hostitele, deaktivuje uživatelské účty a mnoho dalšího
- Maří útoky ještě předtím, než k nim dojde, pomocí špičkových funkcí prevence.

"GravityZone XDR vyniká v propojení a korelaci incidentů v čase, napříč celým naším podnikem, čímž jsme ihned zaznamenali hmatatelnou přidanou hodnotu. Není možné přehlédnout výhody řešení od jednoho dodavatele, s funkcemi detekce out-of-the-box pro identifikaci a vyšetřování známých i neznámých hrozeb, které našim analytikům poskytuje znalosti o tom, jakým způsobem k incidentu došlo, a zároveň nabízí nejlepší způsoby, jak na něj reagovat."

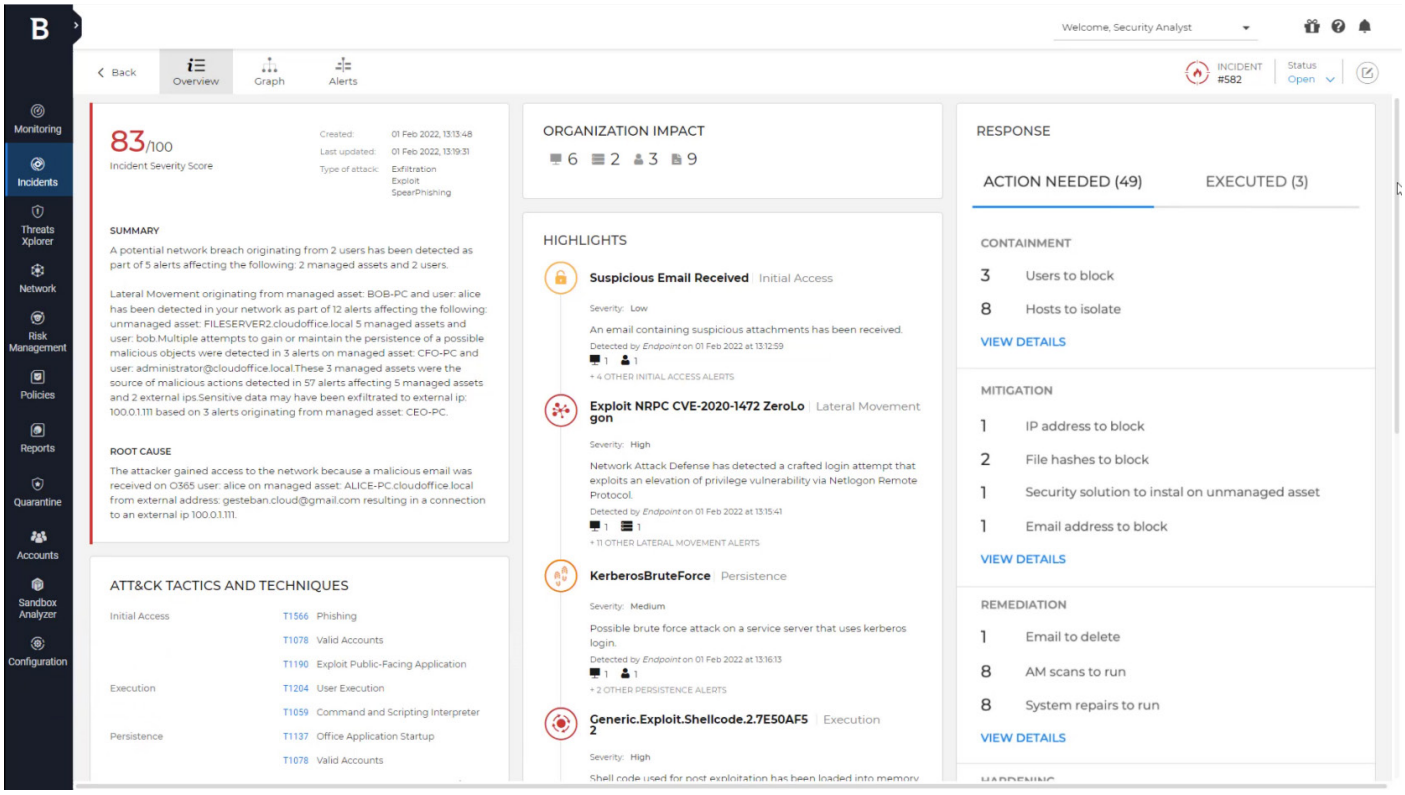
Mahmood Haq, chief information security officer, MyVest

Díky možnostem obsaženým v GravityZone XDR, mají bezpečnostní týmy okamžitý přístup ke korelovaným zdrojům událostí, základním datům a bohatému kontextu, takže mohou rychle identifikovat řetězec akcí spojených s kybernetickými útoky v celém svém prostředí. Pokročilé strojové učení a umělá inteligence systému GravityZone, poskytují bezpečnostním týmům přehled o vzorcích chování, které tak umožňují podniknout smysluplné kroky. Tato technologie minimalizuje riziko falešných pozitivních nálezů, čímž výrazně pomáhá bezpečnostním týmům.

GravityZone XDR shromažďuje data z několika různých systémů:

- On-premises a cloudové koncové body a servery
- Aplikace Microsoft Office 365™ a e-mail
- Cloudové pracovní zátěže, jako jsou např. Amazon Web Services®
- Microsoft® Active Directory® pro správu identit sítě

Všechny bezpečnostní nástroje, pokrývající tato prostředí, lze spravovat z jediné intuitivní konzoly GravityZone.



Obrázek 1: GravityZone XDR poskytuje bezpečnostním týmům podrobné informace o útocích. To umožňuje rychlé pochopení detailů bezpečnostních incidentů a událostí, potenciálního dopadu na organizaci, pravděpodobných klíčových příčin a doporučených opatření.

Jak XDR zlepšuje detekci a reakci

GravityZone XDR podporuje GravityZone Business Security Enterprise s jedním nebo více senzory XDR. GravityZone poskytuje špičkové technologie kybernetické bezpečnosti - ochranu koncových bodů, detekci a reakci, analýzu rizik uživatelů a koncových bodů, obranu proti síťovým útokům, filtrování webového obsahu, vyladěné strojové učení, analýzu sandboxu, flexibilní správu zásad, rozsáhlý reporting a další - prostřednictvím jediné intuitivní konzole pro správu, založené na cloudu. Díky senzorům XDR rozšiřuje Bitdefender své detekční schopnosti i za hranice koncového bodu.

GravityZone XDR podporuje 4 další typy senzorů. Tyto senzory přijímají informace z různých zdrojů, a předávají je pokročilému enginu strojového učení. GravityZone XDR analyzuje data zpracovaná strojovým učením, a sestavuje podrobnou časovou osu útoku, která je prezentována v poradci pro incidenty (Incident Advisor). Díky GravityZone EDR jsou bezpečnostní týmy již schopny provádět zásahy zahrnující izolaci hostitele, nahrávání souborů do sandboxu GravityZone k další analýze, ukončování procesů a otevírání vzdáleného příkazového řádku na koncových bodech. Přidáním každého z uvedených senzorů (viz níže), GravityZone XDR rozšiřuje své možnosti reakce.

Productivity Applications Sensor

Odcizení účtů Microsoft Office 365 je považováno za jednu z největších odměn pro kyberzločince. Ti často používají phishingové útoky, aby vylákali oběti k vyzrazení jejich cenných přihlašovacích údajů k Office 365. Přehled o takovém chování je pro bezpečnostní týmy neocenitelný. GravityZone XDR detekuje útoky na účty a e-maily Office 365, nebo útoky pocházející z těchto účtů a e-mailů.

Productivity Applications Sensor identifikuje specifika účtů Office 365, která mohou být spojena s činností kyberzločinců. Senzor detekuje následující akce:

- Vypnutí ochrany proti phishingu v Office 365.
- Podezřelé chování při vytváření uživatele, například nově vytvořený uživatel vyloučený z požadavků na vícefaktorové ověřování.
- Nahrávání dokumentů s podezřelými makry do služeb SharePoint a OneDrive.
- Nahrávání spustitelných souborů do účtů Office 365.
- Podezřelé požadavky na přístup, například když je uživateli v krátkém časovém úseku umožněn přístup k více souborům nebo adresářům na různých webech SharePoint.

Senzor také detekuje anomálie v chování uživatele, které se odchylují od obvyklé standardní úrovně. Dokáže například identifikovat, kdy uživatel v daném dni prováděl neobvyklý počet administrativních činností nebo manipulací s dokumenty, pokud se tyto činnosti odchylují od běžných postupů uživatelského účtu.

Detekce podezřelého chování Office 365 se vztahuje i na e-maily. Productivity Applications Sensor identifikuje následující podezřelé aktivity uvnitř Microsoft Exchange Online™:

- Exfiltrační e-maily sloužící ke stažení souborů z napadeného uživatelského účtu.
- Spearphishingové e-maily - jejich cílem je oklamat uživatele a přimět ho k vyzrazení přihlašovacích údajů k účtu.
- Podezřelá aktivita s oprávněním k poštovní schránce; například pokud uživatel získal oprávnění k přístupu k několika různým poštovním schránkám v krátkém časovém období.
- Uživatelský účet odstraňující velké množství e-mailů v poštovní schránce, kterou uživatel nevlastní.

Spolu s identifikací tohoto podezřelého chování, pomáhá GravityZone XDR bezpečnostním týmům přijímat opatření na zajištění ochrany jejich organizace. Pomocí senzoru Office 365 mohou bezpečnostní týmy mazat e-maily ze všech organizací Office 365, a pozastavovat účty Office 365. To vše z ovládacího panelu GravityZone.

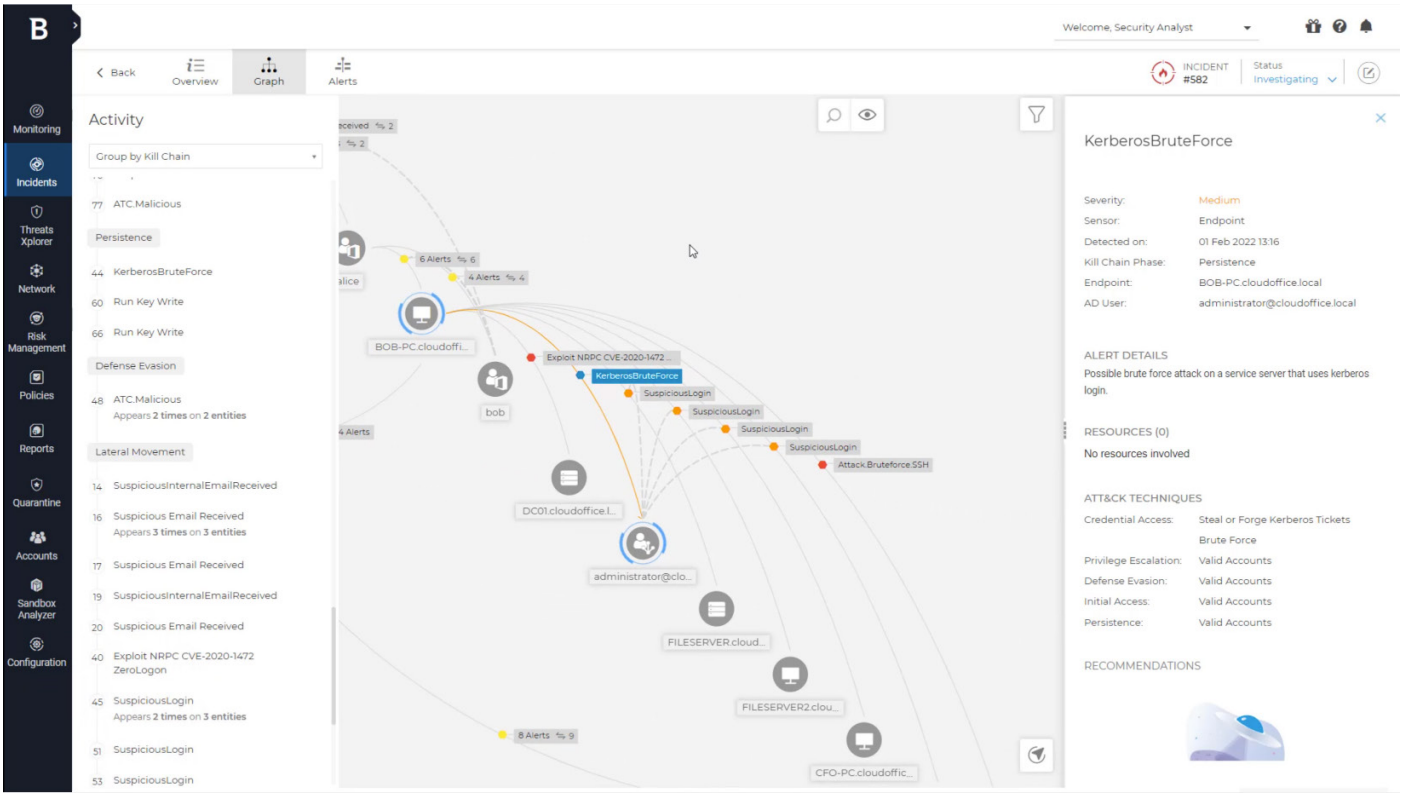
Cloud Sensor

Pomocí senzoru XDR Cloud Sensor monitoruje GravityZone XDR aktivity, které mohou naznačovat, zda bylo ohroženo zabezpečení cloudových prostředí, jako je například Amazon Web Services® (AWS). Senzor sleduje několik indikátorů útoku.

Cloud Sensor rozpoznává anomálie tak, že nejprve stanoví základní linii běžného chování, a poté identifikuje, kdy se zjištěné činnosti od této základní linie odchylují. GravityZone detekuje, když uživatel provede akci mimo tuto základní linii, když byl nahrán soubor s podezřelou příponou a odchyluje se od standardní linie chování, když cloudová úloha provede akci mimo obvyklý rozsah činnosti, a další detekce specifické pro cloud.

Cloud Sensor navíc identifikuje podezřelé aktivity spojené s mnoha podrobnými funkcemi cloudových služeb, jako je například AWS Lambda®. Senzor zjistí, kdy útočník spustil funkci Lambda, která vyvolá podezřelou akci. Dokáže například rozlišit, kdy bylo provedeno podezřelé automatické spuštění kódu, například pomocí funkce Lambda k vytvoření přístupového klíče k backdooru uživatele služby AWS Identity and Access Management (IAM). Dalším příkladem je použití funkce Lambda k aktualizaci bezpečnostní skupiny, která povoluje přístup na určitý port, GravityZone XDR to identifikuje jako manévr, který může útočníkovi umožnit přístup ke cloudové instanci.

GravityZone XDR Cloud Sensor detekuje další podezřelé chování, například když neznámý uživatel nebo hostitel odstraní výchozí šifrování z bucketu S3 (AWS Simple Cloud Storage). Provedením této akce útočník odhalí všechny zašifrované objekty (pomocí šifrování na straně serveru) v tomto bucketu S3. XDR detekuje, když útočník zakáže nebo odstraní monitorovací služby, například zastaví službu protokolování Amazon CloudTrail, nebo odstraní protokoly z monitorovací služby AWS CloudWatch. Identifikuje také, když útočník provádí průzkumné akce proti bucketu S3. GravityZone XDR také dokáže odhalit, kdy se uživatel přihlásil z více oblastí současně, což je typický indikátor napadeného účtu.



Obrázek 2: Bezpečnostní týmy si mohou v rozšířeném zobrazení incidentů prohlédnout podrobné informace o všech aspektech útoku. Naše senzory monitorují a korelují aktivity napříč různými zdroji dat, aby poskytly podrobnosti o každém bodě útoku ve snadno srozumitelném formátu. Aktivitu lze třídit podle času nebo řetězce útoku podle toho, jak bezpečnostní týmy preferují analýzu útoků.

Identity Sensor

Identity Security je zásadním prvkem ,umožňujícím větší kybernetickou odolnost. Identifikace podezřelých autentizačních aktivit pro aplikace, nástroje DevOps, databáze, systémy, cloudová prostředí a další kritické zdroje, pomáhají předcházet nebo zmírňovat potenciální škody, způsobené kybernetickým útokem. Jakmile je Identity Sensor připojen k Active Directory,

detekuje aktivitu spojenou s útoky, které se pokoušejí používat kompromitované účty, tokeny a objekty. To zahrnuje nejen účty koncových uživatelů, ale i systémové účty a účty API.

Identity Sensor detekuje útoky zaměřené na síťový ověřovací protokol Kerberos. Mezi podporované detekce patří schopnost zjistit, kdy je přihlašovací jméno Kerberos použito k provedení útoku hrubou silou na systém. Během útoku hrubou silou se záškodník pokouší použít rychle vygenerovaná hesla nebo šifrovací klíče k získání přístupu do systému. Senzor detekuje také další aktivity, související se systémem Kerberos, včetně použití ukradených ticketů Kerberos k laterálnímu pohybu v síti, požadavku na tickety se slabým šifrováním - což je běžný znak nekalého jednání - a replay útoků. Replay útoky spočívají v krádeži paketů ze sítě za účelem jejich předání službě nebo aplikaci.

Identity Sensor také rozpozná podezřelá přihlášení po detekci útoku hrubou silou. Senzor identifikuje, když útočník zaregistruje podvodný Active Directory Domain Controller a použije jej k injektáži nebezpečných objektů do dalších doménových kontrolérů v rámci stejné infrastruktury Active Directory. Identifikuje, když útočník provádí různé činnosti na objektu Active Directory, a autentizuje se do vzdálených systémů pomocí ukradených pověření.

Výkonnou detekční komponentu GravityZone XDR Identity Sensor doplňují funkce, které umožňují bezpečnostním týmům podniknout relevantní kroky; bezpečnostní týmy mohou například zakázat účet Active Directory nebo vynutit reset hesla přímo z konzoly pro správu GravityZone.

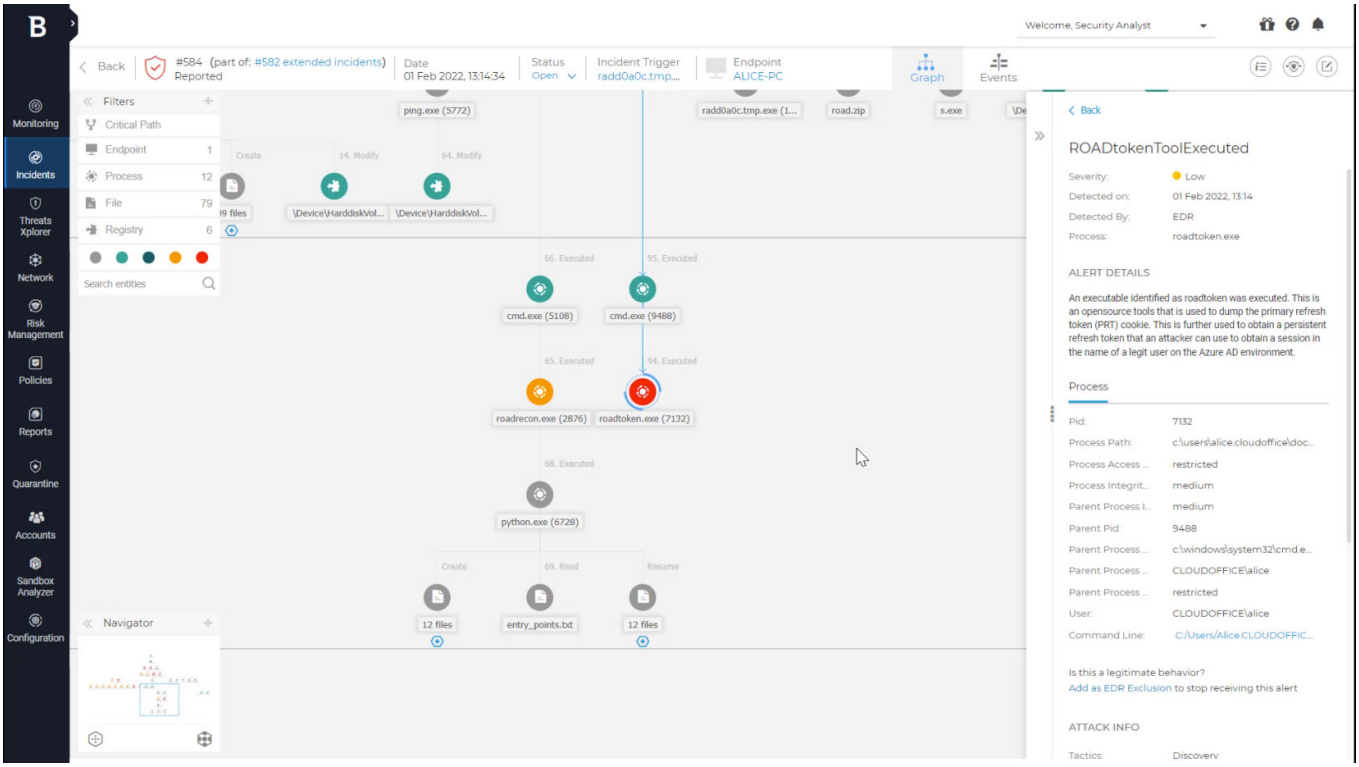
Network Sensor

GravityZone XDR Network Sensor je virtuální zařízení, které monitoruje síťový provoz a hledá příznaky útoku. Záškodníci se často snaží rozšířit svůj útok tím, že se přesouvají napříč firemní sítí z jednoho systému do druhého. Network Sensor pomáhá bezpečnostním týmům identifikovat, kdy se útočník pokouší o laterální pohyb napříč sítí. Dokáže přesně určit, kdy se útočník pokouší exfiltrovat data do míst mimo organizaci. XDR Network Sensor detekuje techniky skenování portů a útoky hrubou silou, vedené sítí.

GravityZone XDR Network Sensor v kombinaci s GravityZone Network Attack Defence - je klíčovou součástí ochrany koncových bodů Bitdefender - pomáhá překazit síťové útoky, a zároveň poskytuje bezpečnostním týmům cenný vizuální přehled, který snižuje dopad kybernetických útoků a celkovou dobu potřebnou k jejich vyřešení.

Bezpečnostní nástroje světové úrovně ve spojení s odbornou expertízou v oblasti zabezpečení

GravityZone XDR poskytuje organizacím kompletní řešení kybernetické bezpečnosti, které kombinuje oceňovanou technologii prevence, se sofistikovanými funkcemi detekce a reakce, které poskytují relevantní informace během kybernetického útoku i po něm. GravityZone XDR podporuje detekci a reakci pro systémy, aplikace pro produktivitu, cloudové pracovní zátěže, identity a sítě, takže se kyberzločinci nemají kde schovat.



Obrázek 3: GravityZone XDR poskytuje podrobné vizualizace útoků, které pomáhají bezpečnostním týmům zkontrolovat průběh každého útoku. Mohou si prohlédnout komplexní analýzu každého jednotlivého souboru zapojeného do útoku, a přijmout opatření k reakci, jako je zařazení souboru na černou listinu, jeho nahrání do sandboxu GravityZone k další analýze, izolace hostitele a další.

Bitdefender
BUILT FOR RESILIENCE

IS4 security s.r.o.
Country Partner Bitdefeder ČR & SK
Jordánská 391, 198 00 Praha 9

Tel.: + 420 245 501 800
email: info@bitdef.cz
web: www.bitdefender.cz

Společnost Bitdefender je lídrem v oblasti kybernetické bezpečnosti, která ve své třídě poskytuje nejlepší řešení prevence, detekce a reakce na hrozby po celém světě. Bitdefender střeží miliony spotřebitelských, podnikových a vládních prostředí, a je jedním z nejdůvěryhodnějších odborníků v oblasti eliminace hrozeb, ochrany soukromí a dat, a zajištění kybernetické odolnosti. Díky rozsáhlým investicím do výzkumu a vývoje objeví laboratoře Bitdefender Labs každou minutu více než 400 nových hrozeb, a denně ověří přibližně 40 miliard dotazů na výskyt hrozeb. Společnost je průkopníkem průlomových inovací v oblasti antimalwaru, zabezpečení IoT, behaviorální analytiky a umělé inteligence, a její technologie si licencuje více než 150 nejuznávanějších světových technologických značek. Společnost Bitdefender byla založena v roce 2001 a má zákazníky ve více než 170 zemích s pobočkami po celém světě.

Více informací najdete na https://www.bitdefender.cz

Bitdefender SSG XDR TechnicalBrief NoPrint NoLocalization DEX59 2 en_EN
CD-04/13/2022 - MD-Apr/13/2022