DATOVÝ LIST

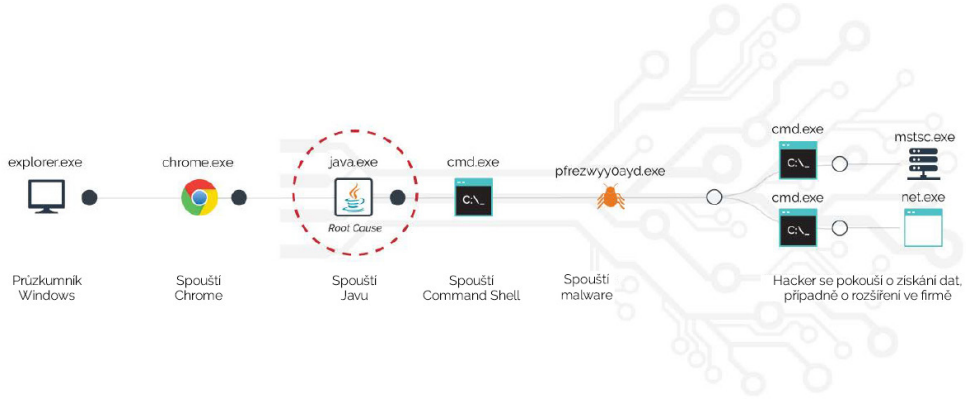
Cb RESPONSE

Rychlejší detekce a reakce

POKROK ÚTOČNÍKŮ JDE DĚSIVÝM TEMPEM

Není možné předem odhalit veškeré škodlivé chování a chránit se proti němu. 93 % průniků napadne první systém[1] během minuty či méně. Je tedy životně důležité je rychle odhalit a zareagovat. Většina bezpečnostních center nemá tak úplný přehled, jaký by potřebovala k rychlému a informovanému rozhodování.

Cokoli, co vám nezajistí 100% přehled, jsou vyhozené peníze. Vznikají tak slepá místa, kvůli nimž nelze odhalit základní příčinu a zabránit budoucím útokům. Jiné produkty pro detekci a reakci na koncových bodech slibují rychlé hledání, ale nemají stoprocentní přehled. Prohledávají tedy neúplné údaje. Jedině Cb Response obsahuje úplnou sadu nástrojů zajišťujících viditelnost všech údajů, rychlou analýzu a vzdálenou nápravu. To znamená nejrychlejší možnou kompletní reakci na bezpečnostní incidenty.



Nechte si graficky znázornit průběh útoku, *takže vždy poznáte základní příčinu a rozsah útoku.*

Cb Response je speciálně určen pro podnikové týmy bezpečnosti a reakce na incidenty. Nabízí přehledné a rychlé uživatelské rozhraní, neomezené ukládání údajů z minulosti a neomezené škálování, díky němuž vyhoví i těm největším společnostem. Tento špičkový nástroj pro odhalování hrozeb a reakci nabízí bezpečnostním centrům tyto funkce:

ÚPLNÝ PŘEHLED AKTIVIT S PRŮBĚŽNÝM CENTRALIZOVANÝM ZÁZNAMEM

- Veškerá aktivita je zachycena díky 100% nepřetržitému záznamu.
- Díky centralizovanému úložišti máte potřebné údaje vždy na dosah ruky.
- Vizualizace úplné sekvence útoku vám umožní vždy odhalit základní příčinu a postup šíření, což urychlí vyšetřování.
- Neomezené ukládání dat umožňuje úplnou kontrolu jakéhokoli útoku v minulosti – bez ohledu na to, jak dávno k němu došlo.

„Díky Cb Response jsme dokázali sestavit kontrolní seznamy a odhalit viry, které jiným kontrolám unikly.“

– bezpečnostní analytik ve společnosti spravující investice

Carbon Black.

VÝHODY

Nejvyšší rychlost reakce
Zajišťuje reakci na hrozby a jejich řešení v reálném čase, takže zkracuje průměrný čas potřebný na reakci na necelých 15 minut

Úplná viditelnost koncových bodů
Zaznamenává veškerou aktivitu, čímž zrychluje reakci na incidenty a umožňuje aktivní odhalování hrozeb

Neomezené uchovávání dat a škálování
Lze škálovat podle potřeb i těch největších instalací. Umožňuje neomezeně uchovávat data a tak splnit zákonné požadavky a vracet se k minulým událostem

Rychlejší vyšetřování
Potřebné informace jsou vždy k dispozici. Nikdy nenarazíte na slepé místo

Důkladné porozumění útoku
Podívejte se, kam útočník pronikl a co tam udělal

Odhalení hrozeb, které jiné obrany přehlédnou
Zkraťte prodlevu odhalení a omezte způsobené škody

Zamezte budoucím útokům
Odhalte základní příčinu a odstraňte bezpečnostní mezery a slepá místa

Ulehčete práci týmu IT
Zbavte se zbytečného obnovování počítačů z diskových obrazů a žádostí o technickou podporu

Optimalizováno pro nasazení uvnitř podniku
Minimální nároky na infrastrukturu – vaše data jsou vaše data

PŘÍKLADY POUŽITÍ

- Preventivní příprava na průniky
- Odhalování útoků
- Ověření a prověření upozornění
- Reakce na incidenty
- Izolace útoku
- Odhalování hrozeb
- Náprava
- Zabránění hrozbám
- Prioritní správa bezpečnostních záplat

REAKCE V REÁLNÉM ČASE:

- Výrazně zkracuje průměrný čas potřebný k reakci na incident ze 78 hodin na méně než 15 minut. [2]
- Zastavuje probíhající útoky karanténou napadených systémů, ukončením procesů a zákazem hashů po celém podniku.
- „Live Response“ (Reakce v reálném čase) umožňuje úplné a vzdálené vyléčení napadených systémů. Požadovanou akci, například získání rozšířených údajů pro vyšetřování nebo spuštění přizpůsobených skriptů, můžete provést z libovolného místa.
- Pomocí informací o základní příčině můžete uzavřít bezpečnostní mezery a zabránit budoucím útokům.

AKTIVNÍ ODHALOVÁNÍ HROZEB

- Rychlejší odhalování nových útoků a odhalování pokročilých metod útoku. K 53 % průniků v roce 2016 nebylo použito malware, což znamená, že je nezbytně důležité dokázat odhalovat hrozby. [3]
- Aktivně odhaluje i ty nejpokročilejší hrozby, které proniknou vaší obranou.
- Využívá otevřená rozhraní API k propojení s vašimi dalšími bezpečnostními systémy, což umožňuje pokročilé korelování útoků.

OSVĚDČENO I VE VELKÉM MĚŘÍTKU

- Vyžaduje jen minimální prostředky a investice do infrastruktury – v 99 % všech podniků lze instalovat do jediného serverového clusteru.
- Díky integraci na klíč a otevřeným rozhraním API systém hladce zapadne i do těch nejsložitějších prostředí.
- Umožňuje prioritní správu bezpečnostních záplat díky těsné integraci s IBN BigFix.

TECHNICKÉ VLASTNOSTI

- Libovolné škálování podle potřeb jakékoliv společnosti
- Neomezené uchovávání údajů z minulosti
- Správa bezpečnostních záplat s určováním priorit pomocí IBM BigFix
- Využívá méně než 1 % výkonu procesoru
- Využívá méně než 20 MB paměti
- Průměrný síťový přenos 50 bytů za sekundu
- Ochrana před útoky typu „man-in-the-middle“ pomocí obousměrného ověřování SSL na serveru
- Centralizovaná správa, ukládání dat a řízení
- 100% otevřená rozhraní API umožňující úplnou integraci

PODPOROVANÉ PLATFORMY

VYŽÁDEJTE SI UKÁZKU

Kontaktujte nás
a domluvte si ukázku.

assistant@freedivision.com

1. MÍSTO V DETEKCI PODLE SPOL. FORRESTER

- Perfektní skóre 5/5 za detekci
- Úplný přehled tak, jak jej bezpečnostní pracovníci potřebují
- Řešení s osvědčenou škálovatelností, které vyhoví jakémukoli podniku
- Podporuje aktivní odhalování hrozeb

The Forrester Wave™: Endpoint Security Suites Report (Zpráva o sadách pro zabezpečení koncových bodů)

Cb RESPONSE POSKYTUJE:

o 75 % rychlejší odhalení základní příčiny

O 90 % menší potřebu obnovovat počítače z diskových obrazů

Údaje o používání produktu partnerem Carbon Black v oblasti reakce na incidenty

[1] 2016 Verizon Data Breach Investigations Report
[2] Údaje o používání produktu partnerem Carbon Black v oblasti reakce na incidenty
[3] 2016 Verizon Data Breach Investigations Report

FREEDIVISION
for safety reasons

O CARBON BLACK

Carbon Black je předním dodavatelem zabezpečení koncových bodů nové generace. Cb Defense, antivirové řešení nové generace (NGAV) od společnosti Carbon Black, využívá převratnou technologii prevence zvanou „Streamovaná prevence“. Díky ní okamžitě odkalí a zastaví kybernetické útoky ještě předtím, než se spustí. Cb Defense představuje jedinečné spojení převratné prevence se špičkovou detekcí a reakcí do jediného nenáročného cloudového nástroje. Carbon Black má více než 2500 zákazníků, z nichž 30 je z žebříčku Fortune 100, a spravuje více než 7 milionů koncových bodů. Tito zákazníci používají Carbon Black jako náhradu starých antivirových programů, k izolaci kriticky důležitých systémů, odhalování hrozeb a k ochraně koncových bodů před nejpokročilejšími kybernetickými útoky včetně těch, které nepoužívají malware.

Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

Telefon: +420 220 972 426
E-mail: info@freedivision.com
www.freedivision.com