Obsah

1 Manažerské shrnutí kybernetické bezpečnosti 2
1.1 Co poskytuje řešení od IcyBear 2
1.2 Proč si vybrat IcyBear jako bezpečnostní řešení? 3
2 Popis nabízeného řešení 4
2.1 Podrobný popis nabízeného řešení pro stanice (Bitdefender Security Enterprise) 4
2.2 Popis řešení Fortinet FORTISIEM 9
2.3 Security Operations Center – SOC 24/7 10
2.4 Check Point Harmony mobile 11
3 Platební a obchodní podmínky 12

1 Manažerské shrnutí kybernetické bezpečnosti

Kybernetická ochrana systémů a informací se stala nedílnou součástí řízení organizace. Je nezbytné chránit pro organizaci cenná informační aktiva (finance, know-how, osobní údaje, procesy, informace o odběratelích a dodavatelích, plnění smluvních nebo zákonných termínů atd.) a vyhnout se tak finančním ztrátám, sankcím a ztrátě důvěry obchodních partnerů a zákazníků.

1.1 Co poskytuje řešení od IcyBear

- Chráníme veškerá Vaše koncová zařízení a body (servery – virtuální, cloudové a fyzické) proti kybernetickým útokům a hackerům 24/7.
- Chráníme Vaše nejcitlivější údaje (mobilní a internetové bankovnictví, digitální osobní identitu, sociální sítě, emaily, hesla, videa, fotky, dokumenty a ostatní soubory).
- Klub kybernetické a digitální bezpečnosti složený z odborníků.
- Nejmodernější technologie a nástroje od více než 4 mezinárodních partnerů.
- Podpora ve formě odborného konzultanta, který Vám pomáhá dohlížet a spravovat kybernetickou bezpečnost.
- Vzdělávání a pravidelný trénink v podobě online kurzů, phishingových kampaní a ebooků.
- Newslettery s upozorněním na největší kybernetické hrozby.
- Možnost získání certifikátu pro zaměstnance o splnění kurzů – Základy kybernetické bezpečnosti.
- Námi vybranou kombinaci bezpečnostních produktů, které zajistí zabezpečení koncových bodů a serverů.
- SOC (Security Operation Centrum) - Naše profesionální týmy v SOC sledují, analyzují a reagují na bezpečnostní události nepřetržitě, aby Vám poskytli ochranu 24/7, která organizacím pomáhá detekovat hrozby, analyzovat je a reagovat na ně dříve, než způsobí škody v provozu firmy.
- 42 vrstev ochrany, která kombinuje celosvětově nejúčinnější platformu pro ochranu koncových bodů s funkcemi detekce a reakce na koncových bodech (EDR), které vám pomohou chránit infrastrukturu koncových bodů (pracovních stanic a serverů) v celém životním cyklu hrozeb, a to s vysokou účinností a efektivitou.
- Hardening založený na analýze rizik. Mechanismus analýzy rizik průběžně vyhodnocuje chybné konfigurace zabezpečení koncových bodů a chování uživatelů, a poskytuje přehledný seznam priorit pro posílení úrovně zabezpečení.
- Patch management, který posiluje zabezpečení, udržujte systémy aktuální a zredukujte složitost IT pomocí automatického záplatování.
- Software pro zabezpečení Vašeho mobilního zařízení nebo tabletu

1.2 Proč si vybrat IcyBear jako bezpečnostní řešení?

Co vše poskytuje IcyBear

Cybersecurity konzultanta

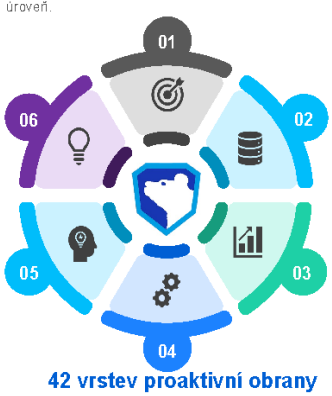
Outsourcing služby in-house vlastního kyberbezpečnostního týmu. Tento odborník se postará o veškeré Vaše otázky a pomůže Vám nastavit kyberbezpečnost ve Vaší firmě na nezbytně nutnou úroveň.

Vzdělávání a trénink

Všem našim členům poskytujeme vzdělávání ve formě on-line kurzů, kde se dozvíte vše nutné o základech kyberbezpečnosti a bezpečném pohybování se v digitálním prostoru. Následně poskytujeme pravidelný trénink – 4x ročně na obranu proti phishingu.

Podporu od komunity odborníků a jejich know-how

Můžete využívat naši podporu ve formě e-mailů, chatu, telefonní podpory a nebo know-how našich odborníků a komunity v reálném čase prostřednictvím platformy Discord a nebo připravovaného vlastního portálu. Dále našim členům pravidelně zasíláme report a informace o největších hrozbách, na které by si měli dát pozor.



42 vrstev proaktivní obrany

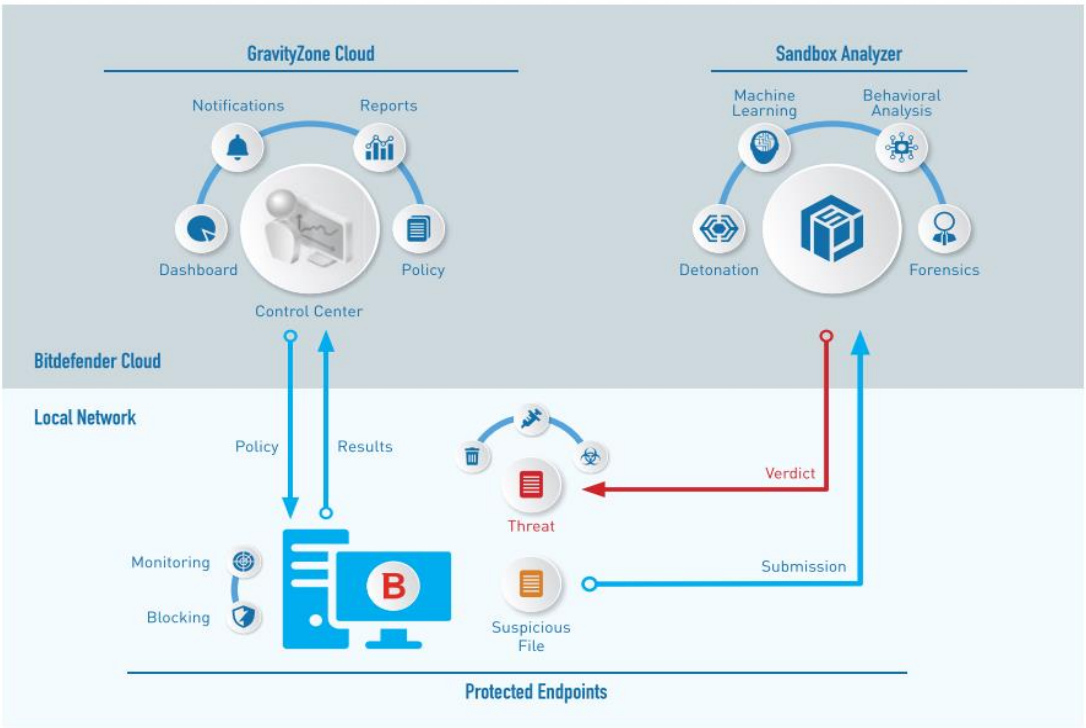
Pro automatizaci kyberbezpečnostních procesů kombinujeme nejúčinnější platformu na světě s ochranou koncových bodů v 42 vrstvách proaktivní obrany, které Vám pomohou dokonale chránit infrastrukturu - pracovní stanice, laptopy, servery, mobilní telefony a tablety.

SOC 24/7 (MDR)

Náš SOC 24/7 (MDR) tým udržuje Vaši organizaci v bezpečí 24x7 pomocí monitorování všech koncových bodů, pokročilé prevence útoků, jejich detekce a proaktivní obrany v reálném čase.

FortiSIEM

FortiSIEM spojuje viditelnost, korelaci, automatickou odezvu a nápravu v jediném, škálovatelném řešení. Snižuje složitost správy síťových a bezpečnostních operací, aby se efektivně uvolnily zdroje, zlepšila se detekce narušení a narušení se zabránilo.



2 Popis nabízeného řešení

Řešení IcyBear obsahuje vždy nejlepší kombinaci zabezpečení nové generace pro všechny typy chytrých zařízení, počítačů, notebooků, serverů (fyzických, cloud, virtuálních). Technologie jsou přidávány a upravovány podle aktuální situace na trhu kybernetické bezpečnosti a s ohledem na nejnovější trendy a aktuální hrozby.

Níže popsané technologie jsou použity jako software přímo u klienta nebo v datovém centru IcyBear pro aktivní dohled a vyhodnocování bezpečnostních incidentů.

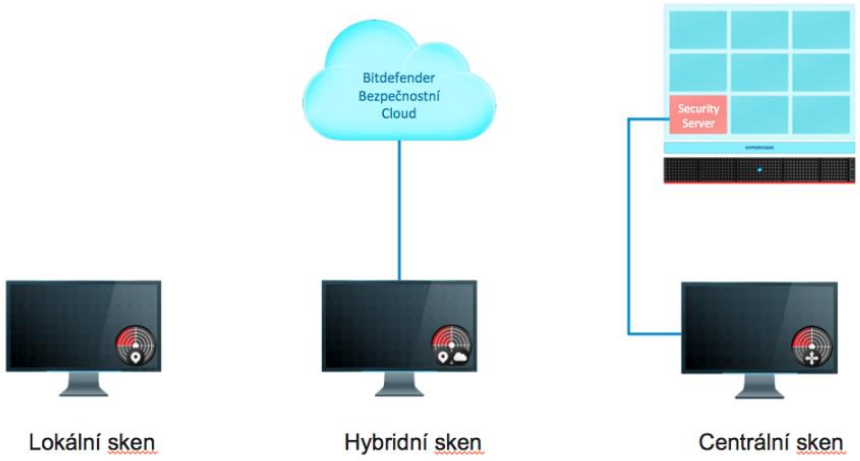
2.1 Podrobný popis nabízeného řešení pro stanice (Bitdefender Security Enterprise)

Bitdefender Security Enterprise (dále jen BDSE) je firemní řešení nabízející nasazení centrální správy všech zařízení ve variantách on-premise (hostované u zákazníka) nebo hostované v cloudu. BDSE umožňuje spravovat fyzické, virtuální a mobilní koncové body nezávisle na operačním systému, hypervizoru, a to vše z jediné centrální konzoli správy. BDSE řešení se neinstaluje, ale pouze konfiguruje díky využití principu virtuální appliance ihned připravených k provozu. Řešení je plně škálovatelné od jednotek až po nekonečně mnoho chráněných zařízeních využitím systému klonování virtuálních appliancí.

Hlavní technologie, které řadí BDSE dle nezávislých testů dlouhodobě mezi nejlepší firemní řešení jsou: antivirus a antimalware s behaviorální monitoringem, ochrana před hrozbami nultého dne pomocí globální ochranné sítě BDSE, kontrola aplikací a sandboxing, firewall, kontrola zařízení, kontrola obsahu s antiphishingem a antispamem pro mailservery.

BDSE nabízí vzdálenou instalaci na neomezené množství stanic včetně automatické odinstalace většiny známých konkurenčních antimalwarových řešeních.

BDSE umožňuje kromě klasického i lokální skenování a testování souborů, aplikací, paměti a registrů na hrozby ve variantách hybridního a centrálního skenování. V případě hybridního skenování je umožněno přenést částečně zátěž z lokálních zdrojů koncového bodu do globální ochranné sítě Bitdefenderu. V případě centrálního skenování se využívá specializovaných bezpečnostních virtuálních serverů (Security Server), které se o tyto procesy starají. Tyto bezpečnostní virtuální appliance centralizují a deduplikují antimalwarové procesy.



Výhody řešení

BDSE nabízí na rozdíl od konkurenčních řešení 4 vrstvy bezpečnosti:

- Ochrana na bázi signatur.
- Sandbox B-HAVE.
- ATC pokročilá ochrana před hrozbami.
- Globální síť ochrany (Nimbus, která je dostupná v rámci centrálního serveru).

Globální síť ochrany využívá více než 100 různých webových služeb k behaviorální analýze probíhajících útoků, včetně zjišťování korelací mezi nimi. Na Globální síť ochrany je napojeno více než 500 milionů koncových bodů. Využívá rychlou nerelační databázi MongoDB a garantuje imunizaci všech připojených koncových bodů maximálně do 3 sekund. Dokáže garantovat zjištění spamových vln kdekoliv na světě do 10 sekund.

Další výhody:

- Jeden typ agenta instalovaného na koncové stanice schopného se přizpůsobit danému typu koncové stanice a jejímu operačnímu systému.
- Platforma nezávislá na hypervizoru (Hyper-V, Vmware, Citrix, KVM) a umožňující plnou integraci s více AD, Vmware vCenter, Citrix XenServer prostředími.
- Možnosti nasazení agentů na jednotlivé stanice vzdáleně nebo lokálně.
- Možnost nastavení uživatelů s granulárními přístupovými právy do příslušných skupin koncových stanic včetně nastavení plně nastavitelných rolí.

Funkční vlastnosti řešení

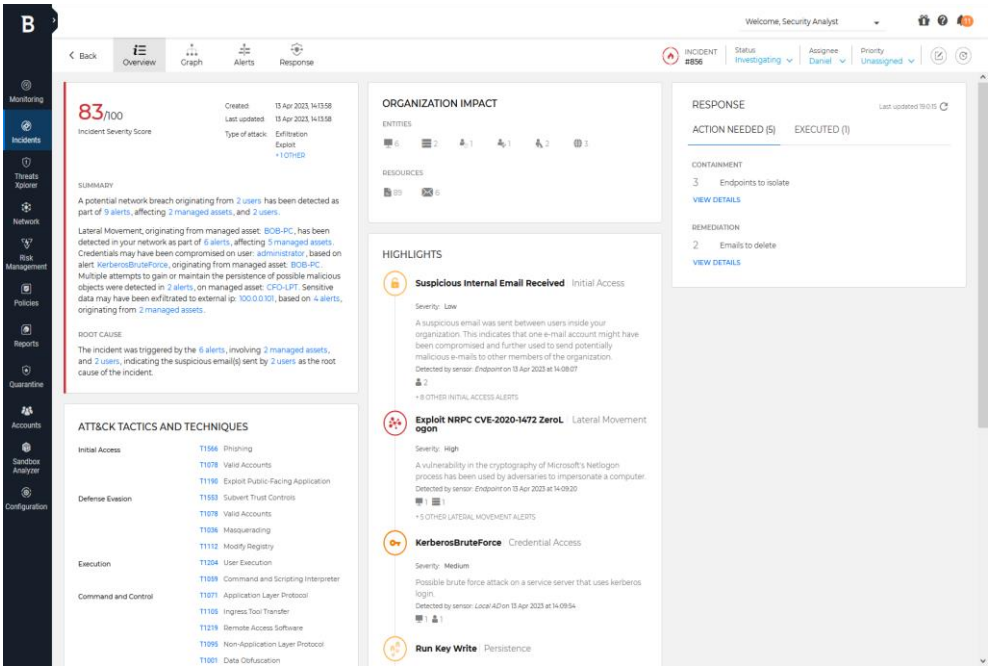
Souhrn technických částí a funkcí řešení BDSE

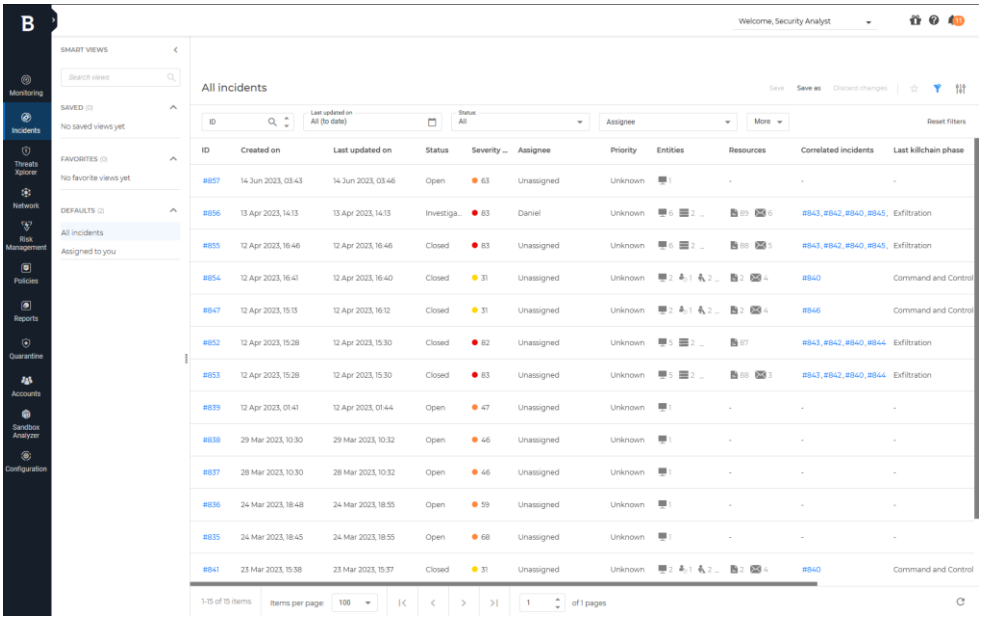
BDSE nabízí následující funkční vlastnosti, které jsou plně v souladu s požadavky ZD:

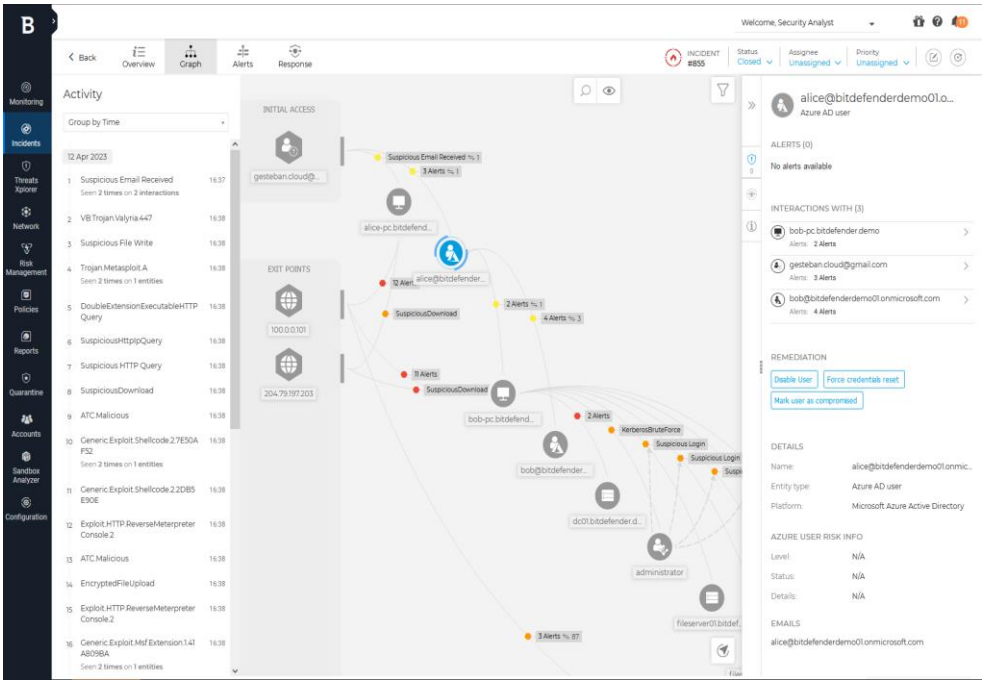
- Nastavení pravidelných naplánovaných skenů.
- Nastavitelné pravidelné aktualizace signatur a produktů.
- Pokročilý reporting včetně logování.
- Automatické upozorňování nejen na malwarové události.
- Plně nastavitelné místa lokací pro aktualizace, centrální sken, komunikační přenos.
- Možnosti detailního nastavení chování klienta na koncovém bodu (silent mode, power user, nastavení hesla pro odinstalaci).
- Detailní nastavení pravidel pro firewall včetně nastavení chování dle aktuálně připojené sítě.
- Import/export politik.
- Advanced Threat Control (ATC).
- Intrusion detection systém (IDS).
    - Sleduje datové toky, hledá v nich pokusy o útok a ty poté zastavuje tak, aby nedošlo k přerušení jiné komunikace. Systém využívá vlastní pravidelně aktualizovanou databázi a umožňuje customizace nastavení, případně výběr použití pouze konkrétních pravidel.
- Možnost detailního nastavení přístupových práv uživatelů.
- Skenování externích zařízení.
- Možnosti vytváření upravitelných instalačních balíčků.
    - Silent instalace – produkt umožňuje tzv. bezodpovědní instalace.
    - Plná podpora vzdálených instalací, která probíhá přes Windows Management Instrumentation, což je součástí všech operačních systémů Windows.
- Možnosti upravení již nainstalovaných instalačních balíčků.
- Možnost nastavení prověřovaných přípon souborů pro veškeré antimalware procesy.
- Možnost nastavení výjimek pro veškeré antimalware procesy.
- Aplikační kontrola.
    - Kontrola a povolení nebo blokování aplikací s využitím největší, interní, pravidelně aktualizované databáze aplikací s možností přidávat své vlastní a to manuálně (procházením disku) nebo automaticky s využitím klientské. Kontrola aplikací probíhá

zpravidla na základě kontrolního součtu, jména aplikace, cesty na datovém médiu, vnitřní databáze, různých kombinací a dalších v závislosti na konfiguraci.

- Kontrola webového přístupu.
- Ochrana dat před opuštěním organizace.
- Kontrola zařízení (USB, DVD, Bluetooth, Wi-fi...) včetně whitelistu a blacklistu.
- Antiphishing engine.
- Antispam engine.
- Antiransomware engine.
- Anti-malware engine.
    - Na základě signatur (znalostní databáze) a detekce podezřelého chování (heuristika).
    - Zero-day attack – ochrana proti útokům a škodlivým kódům, které ještě nejsou známé.




Welcome, Security Analyst
SMART VIEWS
Search views
SAVED (0)
No saved views yet
FAVORITES (0)
No favorite views yet
DEFAULTS (2)
All incidents
Assigned to you
Monitoring
Incidents
Threats Xplorer
Network
Risk Management
Policies
Reports
Quarantine
Accounts
Sandbox Analyzer
Configuration
All incidents
Save
Save as
Discard changes
Reset filters
Last updated on
All (to date)
Status:
All
Assignee
More
ID
Created on
Last updated on
Status
Severity ...
Assignee
Priority
Entities
Resources
Correlated incidents
Last killchain phase
#857 14 Jun 2023, 03:43 14 Jun 2023, 03:46 Open 63 Unassigned Unknown -
#856 13 Apr 2023, 14:13 13 Apr 2023, 14:13 Investiga... 83 Daniel Unknown #843, #842, #840, #845 Exfiltration
#855 12 Apr 2023, 16:46 12 Apr 2023, 16:46 Closed 83 Unassigned Unknown #843, #842, #840, #845 Exfiltration
#854 12 Apr 2023, 16:41 12 Apr 2023, 16:40 Closed 31 Unassigned Unknown #840 Command and Control
#847 12 Apr 2023, 15:13 12 Apr 2023, 16:12 Closed 31 Unassigned Unknown #846 Command and Control
#852 12 Apr 2023, 15:28 12 Apr 2023, 15:30 Closed 82 Unassigned Unknown #843, #842, #840, #844 Exfiltration
#853 12 Apr 2023, 15:28 12 Apr 2023, 15:30 Closed 83 Unassigned Unknown #843, #842, #840, #844 Exfiltration
#839 12 Apr 2023, 01:41 12 Apr 2023, 01:44 Open 47 Unassigned Unknown -
#838 29 Mar 2023, 10:30 29 Mar 2023, 10:32 Open 46 Unassigned Unknown -
#837 28 Mar 2023, 10:30 28 Mar 2023, 10:32 Open 46 Unassigned Unknown -
#836 24 Mar 2023, 18:48 24 Mar 2023, 18:55 Open 59 Unassigned Unknown -
#835 24 Mar 2023, 18:45 24 Mar 2023, 18:55 Open 68 Unassigned Unknown -
#841 23 Mar 2023, 15:38 23 Mar 2023, 15:37 Closed 31 Unassigned Unknown #840 Command and Control
1-15 of 15 items
Items per page: 100
1
of 1 pages


Welcome, Security Analyst
Back
Overview
Graph
Alerts
Response
INCIDENT #855
Status Closed
Assignee Unassigned
Priority Unassigned
Activity
Group by Time
12 Apr 2023
1 Suspicious Email Received 16:37
Seen 2 times on 2 interactions
2 VB.Trojan.Valyria.447 16:38
3 Suspicious File Write 16:38
4 Trojan.Metasploit.A 16:38
Seen 2 times on 1 entities
5 DoubleExtensionExecutableHTTP Query 16:38
6 SuspiciousHttpIpQuery 16:38
7 Suspicious HTTP Query 16:38
8 SuspiciousDownload 16:38
9 ATC.Malicious 16:38
10 Generic.Exploit.Shellcode.2.7E50AF32 16:38
Seen 2 times on 1 entities
11 Generic.Exploit.Shellcode.2.2DB5E90E 16:38
12 Exploit.HTTP.ReverseMeterpreterConsole.2 16:38
13 ATC.Malicious 16:38
14 EncryptedFileUpload 16:38
15 Exploit.HTTP.ReverseMeterpreterConsole.2 16:38
16 Generic.Exploit.Msf.Extension.1.41A809BA 16:38
Seen 2 times on 1 entities
INITIAL ACCESS
EXIT POINTS
100.0.0.101
204.79.197.203
alice@bitdefenderdemo01.o...
Azure AD user
ALERTS (0)
No alerts available
INTERACTIONS WITH (3)
bob-pc.bitdefender.demo
Alerts: 2 Alerts
gesteban.cloud@gmail.com
Alerts: 3 Alerts
bob@bitdefenderdemo01.onmicrosoft.com
Alerts: 4 Alerts
REMEDIATION
Disable User
Force credentials reset
Mark user as compromised
DETAILS
Name: alice@bitdefenderdemo01.onmic...
Entity type: Azure AD user
Platform: Microsoft Azure Active Directory
AZURE USER RISK INFO
Level: N/A
Status: N/A
Details: N/A
EMAILS
alice@bitdefenderdemo01.onmicrosoft.com

2.2 Popis řešení Fortinet FORTISIEM

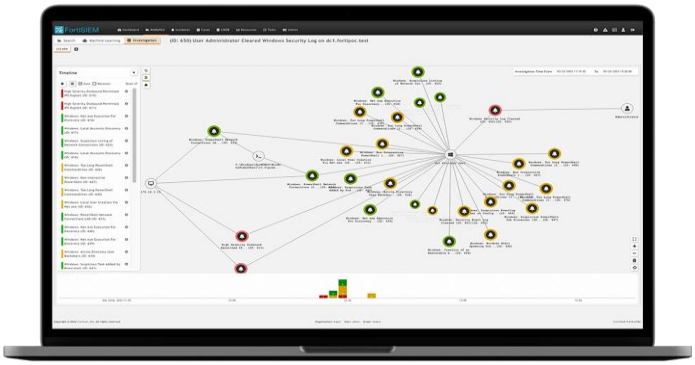
Fortinet je přední bezpečnostní informační správa událostí (SIEM). Tato platforma monitoruje a analyzuje události v reálném čase. Tím nám poskytuje kompletní přehled o aktivitách v síti a umožňuje nám identifikovat a reagovat na bezpečnostní incidenty včas. Díky svému pokročilému korelačnímu enginu a automatizovaným procesům přispívá ke snížení rizika a zajišťuje, že žádná hrozba nezůstane nepovšimnuta.

FortiSIEM je navržen tak, aby byl páteří vašeho bezpečnostního provozního týmu a poskytoval možnosti od automatického vytváření inventáře aktiv až po použití nejmodernější behaviorální analýzy k rychlé detekci a reakci na hrozby. FortiSIEM je jediná bezpečnostní operační platforma v oboru s plně vestavěnou databází správy konfigurace (CMDB).

Díky své CMDB může FortiSIEM automaticky využívat aktivní a pasivní metody zjišťování k vytvoření inventáře vašeho digitálního majetku. To zahrnuje zařízení a jejich aplikace a sleduje stav těchto aktiv v průběhu času. Průběžné shromažďování kontextu, jako jsou konfigurace, výkon, zranitelnost, jejich vztah k obchodním službám a jejich přidružení OT modelu Purdue, aby týmy věděly o stavu prostředí, když dojde k incidentu. A mají viditelnost potřebnou k proaktivnímu řešení problémů.

Experti na analýzu hrozeb z laboratoří FortiGuard pracují 24 hodin denně, 7 dní v týdnu, aby analyzovali nejnovější hrozby a extrémně rychle vytvořili opravné patche. V kombinaci s nejnovějšími schopnostmi detekce anomálií chování řízených umělou inteligencí, jako je UEBA, FortiSIEM chrání před známými i neznámými hrozbami. Statistické modely se využívají k zachycení odchylek, jak podivných, tak nemožných, jako je přihlášení napříč zeměpisnými oblastmi, které by vyžadovalo rychlost superhrdinů (nebo odcizené přihlašovací údaje).

FortiSIEM spojuje viditelnost, korelaci, automatickou odezvu a nápravu v jediném, škálovatelném řešení. Snižuje složitost správy síťových a bezpečnostních operací, aby se efektivně uvolnily zdroje, zlepšila se detekce narušení a dokonce se narušení zabránilo. Pro účinnější vyhledávání hrozeb nyní FortiSIEM obsahuje novou technologii link graph, která umožňuje snadnou vizualizaci vztahů mezi uživateli, zařízeními a incidenty.



2.3 Security Operations Center – SOC 24/7

zajišťuje komplexní centralizaci řízení bezpečnostních událostí a incidentů v jednom bodě s cílem minimalizovat reakční doby na incident a škod z něj plynoucích. Bezpečnostní operační centrum stojí na pilířích přípravy, detekce, analýzy, investigace, reakce a post incident aktivit.

Kontinuálním monitoringem v reálném čase identifikujeme, případně přijmeme, notifikaci o potenciálně škodlivém chování v chráněné infrastruktuře – **detekce**. Určíme, zda se jedná o bezpečnostní událost, nebo o bezpečnostní incident, který může mít negativní dopad na chráněnou infrastrukturu – **analýza**.

Cílem zkoumání daného bezpečnostního incidentu je zjistit konkrétní dopady a cestu, kterou se útočníkovi podařilo proniknout do infrastruktury – **investigace**. Okamžitou reakcí minimalizuje dopad bezpečnostních incidentů – **reakce**. Po úspěšné reakci je zajištěno poučení se z incidentu (kontinuální zlepšování), kontrolu zavedení nápravných opatření a reporting zjištěných skutečností pro zvýšení informovanosti – **post incident aktivity**. To vše díky silné kombinaci **procesů**, **technologií** a **lidských zdrojů** přímo optimalizovaných pro zákazníkovy potřeby.

VÝHODY

+ **Snížení reakční doby na incident (zvýšení efektivity) a tudíž zmírnění dopadu incidentu (snížení nákladů na obnovu).**
+ **Centralizace bezpečnosti** do jednoho bodu.
+ **Real-time znalost** bezpečnostní situace v infrastruktuře.
+ **Snížení nákladů na lidský faktor** (operátoři SOC namísto techniků pro jednotlivé technologie).
+ Minimalizace možnosti pochybení operátorů (**automatizace bezpečnosti**) díky předem definovaným postupům řešení incidentů.
+ Reflexe aktuálních, ale i nově vznikajících hrozeb (**pokrytí komplexního portfolia bezpečnostních hrozeb**).

2.4 Check Point Harmony mobile

Check Point Harmony mobile, chrání uživatele před všemi kybernetickými hrozbami, ať už jde o pokus o phishing, škodlivou přílohu e-mailu, nebo zero-day ransomware, a to napříč všemi vektory útoku. Díky revoluční umělé inteligenci a nejrozsáhlejší síti na sledování hrozeb v oboru dokáže Harmony zastavit útoky ještě předtím, než k nim dojde.

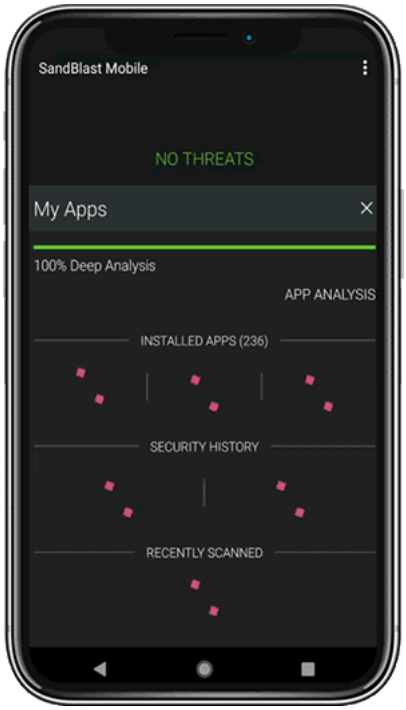
Se vzdálenými uživateli, kteří se připojují k firemním aplikacím odkudkoli, se stále více rozšiřuje prostor pro útoky na vaši organizaci.

Check Point Harmony mobile je první jednotné bezpečnostní řešení pro uživatelská zařízení a přístupy. Chrání zařízení a internetová připojení před nejsofistikovanějšími útoky a zároveň zajišťuje přístup k firemním aplikacím na principu nulové důvěry.

Check Point Harmony mobile umožňuje analýzy zranitelností operačního systému, pokročilých funkcí pro zařízení značky Samsung anebo snadné správy kontroly HTTPS.

Ochrana proti škodlivým souborům využívá službu Check Point Threat Cloud, která skenuje stahované soubory a analyzuje potenciálně škodlivé chování. Pokud je detekováno nějaké riziko, stahování je zablokováno a škodlivý soubor se do zařízení nikdy nedostane.

Na telefonech se systémem Android může Harmony Mobile skenovat soubory v úložišti mobilního zařízení a v případě odhalení škodlivého souboru upozorní uživatele i správce. Uživateli bude doporučeno, aby soubor odstranil, a správce se může rozhodnout omezit přístup zařízení k podnikovým zdrojům.



3 Platební a obchodní podmínky

1. Faktura bude splatná ve lhůtě 3 dnů ode dne jejího doručení a bude vystavena se všemi náležitostmi daňového dokladu, pokud nebude dohodnuto jiným způsobem.
2. Faktura bude vystavena jednorázově po obdržení potvrzení objednávky emailem nebo po online objednání prostřednictvím www stránek icybear.io.
3. Firma není plátcem DPH.
4. Služby budou zahájeny do 3 dnů od obdržení platby.
5. Poskytovatel a Zadavatel se zavazují považovat informace o skutečnostech, o kterých se dověděli na základě plnění této obchodní spolupráce dle Předmětu nabídky za důvěrné a zavazují se zachovat mlčenlivost o takovýchto skutečnostech, a to až do doby, kdy se tyto informace stanou obecně známými a za předpokladu, že se tak nestane porušením povinnosti mlčenlivosti.
6. Obě strany se zavazují, že tyto skutečnosti jiným subjektům nesdělí, nezpřístupní, ani nevyužijí pro sebe nebo pro jinou osobu. Zavazují se zachovat tyto skutečnosti v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům, kteří jsou pověřeni plněním výše zmíněné obchodní spolupráce dle Předmětu nabídky a z tohoto titulu oprávněni se těmito skutečnostmi v nezbytném rozsahu seznámit. Obě strany se současně zavazují zabezpečit, aby i tyto osoby považovaly skutečnosti tvořící obchodní tajemství za důvěrné a zachovávaly o nich mlčenlivost.
7. Poskytovatel neodpovídá za vadné plnění svých závazků, způsobené okolnostmi vylučujícími odpovědnost, jak jsou definovány v obchodním zákoníku.
8. Poskytovatel odpovídá za škodu způsobenou Objednateli v důsledku zaviněných porušení svých smluvních závazků. O odpovědnosti Poskytovatele za způsobenou škodu a o výši způsobené škody, dle rozsahu, uvedeného v tomto ustanovení, rozhodne, nedohodnou-li se smluvní strany jinak, soud.
9. Poškozená smluvní strana nemá nárok na náhradu škody, pokud nesplnění povinností povinné smluvní strany bylo způsobeno zaviněným jednáním poškozené smluvní strany.
10. Právní vztahy neupravené těmito obchodními podmínkami se řídí ustanoveními zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů a dalšími obecně závaznými právními předpis.
11. Užívání produktů se řídí podmínkami souvisejícími s poskytováním produktů Poskytovatele, jako jsou obchodní podmínky, servisní podmínky, EULA a další dokumenty uvedené na adrese https://icybear.io/produktove-podminky/ (dále také „Produktové podmínky“).

Přehled dodávaných bezpečnostních licencí:

Název bezpečnostního software	**Platnost licence**
Bitdefender Endpoint Security Enterprise – Ochrana pro koncové body	Legacy – neomezeně, Fortune a Treasure – 5 let, Spark edice 12 měsíců
Bitdefender Patch management	Legacy – neomezeně, Fortune a Treasure – 5 let, Spark edice 12 měsíců
Check Point Harmony Mobile	Mobile edice 12 měsíců
IcySOC v režimu 5x8 podpora, v režimu 7x24 AI sledování incidentů a proaktivní ochrana	Legacy – neomezeně, Fortune a Treasure – 5 let, Spark, Cube a Mobile edice 12 měsíců
Přístup ke vzdělávání kybernetické bezpečnosti	Legacy – neomezeně, Fortune a Treasure – 5 let, Spark edice 12 měsíců