Bitdefender

DESCRIEREA SOLUȚIEI

Managed Detection and Response (MDR+SOC)

Trusted. Always.

Cuprins

Introducere în Managed Detection and Response

Nevoia de MDR

În peisajul actual al amenințărilor cibernetice care evoluează rapid, organizațiile se confruntă cu provocări de securitate din ce în ce mai complexe și mai sofisticate. Măsurile tradiționale de securitate nu mai sunt suficiente pentru a vă proteja împotriva tacticilor în continuă schimbare folosite de atacatorii cibernetici. Pentru a detecta, răspunde și atenua în mod eficient aceste amenințări, companiile au nevoie de o experiență vastă în analize de securitate și threat hunting, dar se confruntă cu provocări semnificative în recrutarea personalului pentru aceste posturi.

Stabilirea unui centru de operațiuni de securitate (SOC) la nivel intern și angajarea de analiști calificați poate fi o sarcină descurajantă, care consumă multe resurse. Expertiza în domeniul securității cibernetice este limitată, foarte căutată și adesea presupune costuri foarte mari sau pur și simplu nu este disponibilă pentru multe organizații, în special pentru IMM-uri. Serviciile Managed Detection & Response (MDR), pe de altă parte, le oferă organizațiilor o echipă de analiști de securitate cu experiență, cu o cunoaștere aprofundată asupra peisajului amenințărilor, metodologiile de atac și tehnicile de răspuns la incidente. Prin această expertiză, companiile pot beneficia de cele mai recente informații și îndrumări, fără povara recrutării și a formării interne și la un cost mai redus.

Definiția MDR

În contextul în care infractorii cibernetici creează în mod constant noi vectori de atac și exploatează vulnerabilități, serviciile MDR integrează tehnologii de ultimă oră, cum ar fi machine learning, inteligența artificială și analiza comportamentală. Aceste instrumente puternice le permit serviciilor MDR să detecteze în mod proactiv și să răspundă atât amenințărilor cunoscute, cât și celor necunoscute în timp real, oferind companiilor o apărare solidă împotriva riscurilor cibernetice emergente.

În plus, serviciile MDR oferă funcționalități continue de monitorizare și detecție, cu echipe de securitate dedicate, care operează 24x7. Analizând în mod constant traficul de rețea, jurnalele de sistem și datele de la nivel de endpoint, serviciile MDR pot identifica cu promptitudine anomaliile, activitățile suspecte sau semnele unei posibile breșe de securitate. Această monitorizare proactivă asigură detecția și remedierea rapidă a incidentelor de securitate, minimizând timpul de infiltrare al atacatorilor și reducând daunele potențiale cauzate.

De asemenea, serviciile MDR permit o abordare cuprinzătoare a securității cibernetice. Pe lângă detecția avansată a amenințărilor, acestea le oferă organizațiilor servicii complete de răspuns și remediere în cazul producerii unor incidente. În cazul unui incident de securitate, echipa MDR se ocupă de procesul de răspuns la incidente. Serviciile MDR investighează evenimentele de securitate din momentul în care acestea sunt identificate, determinând cauza principală, luând măsuri de izolare și eradicare a amenințării și oferindu-i clientului recomandări despre cum să prevină atacurile în viitor. Scopul MDR este de a gestiona un eveniment sau incident de securitate și de a elimina sau reduce impactul asupra clienților rapid și eficient.

Cele mai bune servicii MDR integrează și o echipă dedicată de threat intelligence, care joacă un rol esențial în îmbunătățirea eficienței și eficacității serviciului în ansamblul său. Echipa de threat intelligence monitorizează continuu peisajul amenințărilor în evoluție, analizează tehnicile de atac emergente și adună informații utile pentru a identifica potențialele amenințări și vulnerabilități. Valorificând acest set de informații cuprinzătoare despre amenințări, un serviciu MDR poate identifica proactiv și poate ierarhiza incidentele de securitate, le poate transmite clienților alerte relevante și în timp util și oferă îndrumări proactive pentru a-și îmbunătăți postura de securitate.

Prin externalizarea responsabilităților de detecție a amenințărilor, monitorizare și răspuns la incidente către furnizorii de servicii MDR, organizațiile se pot concentra asupra operațiunilor lor de bază. Acest lucru le permite echipelor interne

să se concentreze asupra obiectivelor lor principale și să se bazeze în același timp pe expertiza și tehnologiile oferite de serviciile MDR pentru a gestiona operațiunile de securitate de zi cu zi. Serviciile MDR pot ajuta organizațiile mari care au deja o echipă internă responsabilă de operațiunile de securitate, suplimentând capacitatea existentă cu funcțiile oferite de serviciile MDR.

Furnizarea de servicii MDR poate crea avantaje și pentru furnizorii de servicii administrate (MSP). Furnizorii care doresc să-și extindă portofoliul și să le ofere clienților lor soluții complete de securitate cibernetică și expertiză obțin numeroase avantaje prin crearea unui parteneriat MDR. Prin integrarea serviciilor MDR în ofertele lor, aceștia le pot oferi clienților multe dintre beneficiile descrise în acest ghid. Ei pot să îmbunătățească postura de securitate a clienților, să-și consolideze parteneriatul, devenind un consilier de încredere în probleme de securitate cibernetică și să se diferențieze pe piață, oferind o abordare cuprinzătoare și proactivă a securității cibernetice. În plus, serviciile MDR oferă fluxuri de venituri recurente, deoarece acestea implică adesea monitorizare și asistență continuă, ducând la relații pe termen lung cu clienții și oportunități sporite de dezvoltare a companiei.

Acest ghid de soluții va aborda în detaliu serviciile Bitdefender MDR, subliniind beneficiile, caracteristicile și considerentele de avut în vedere de către companiile care doresc să-și îmbunătățească postura de securitate cibernetică și să atenueze riscurile asociate cu peisajul amenințărilor în continuă schimbare.

Servicii Bitdefender MDR

Serviciul Bitdefender MDR pune la dispoziție resursele umane, procesele și tehnologiile necesare pentru a îndeplini toate nevoile dumneavoastră de securitate și a vă oferi rezultatele dorite. Soluțiile EDR/XDR moderne necesită analiști calificați, care să monitorizeze în mod continuu mediul, pe fondul unui număr tot mai mare de alerte, și să-și asume răspunderea pentru fluxurile de răspuns atunci când fiecare secundă contează. Bitdefender MDR își asumă răspunderea pentru aceste aspecte, astfel încât echipele IT și de securitate din cadrul organizației dumneavoastră să se poată concentra pe acțiuni care contribuie la dezvoltarea afacerii.

Beneficii principale

- **Analiști, nu doar alerte –** Bitdefender MDR gestionează întregul ciclu de viață al alertelor, analizând mii de alerte pentru a le reduce la doar câteva răspunsuri și recomandări. Vedeți totul în mod transparent în portalul MDR și primiți notificări doar despre ceea ce este important pentru dumneavoastră.
- **Răspuns rapid și decisiv –** analiștii noștri de securitate evaluează rapid incidentele de securitate și iau măsuri decisive pentru a limita și a atenua amenințările, printr-o gamă largă de acțiuni aprobate în prealabil.
- **Cea mai bună platformă de securitate –** serviciul Bitdefender MDR include platforma noastră de securitate de top în industrie, care se plasează în mod constant pe locul 1 la testele independente realizate de MITRE®, AV-Test© și AV-Comparatives©. În plus, Bitdefender este deținătoarea platformei, oferindu-le clienților noștri un singur stack de tehnologii de securitate pe baza căruia să își consolideze apărarea.

Prezentare generală a serviciilor

Componentă servicii	Bitdefender MDR	Bitdefender MDR PLUS
Cea mai bună platformă de securitate din industrie	✓	✓
SOC disponibil 24x7	✓	✓
Acțiuni pre-aprobate (PAA)	✓	✓
Threat Hunting	✓	✓
Recomandări de la experți	✓	✓
Analiza cauzei și impactului incidentului	✓	✓
Portal MDR și funcționalități de raportare	✓	✓
Integrarea de servicii profesionale	✓	✓
Asigurarea în cazul producerii unei breșe de securitate cibernetică	✓	✓
Administrator de cont pe probleme de securitate disponibil 24x7 (Customer Success)		✓
Fluxuri de threat intelligence și analiza globală a acestor date		✓
Monitorizare pentru Dark Web		✓
Security Baselining de bază în domeniul securității și crearea de modele personalizate ale amenințărilor		✓
Protecția mărcii și IP-ului		✓
Monitorizarea țintelor de importanță majoră		✓
Senzori XDR	Add-on-uri	Add-on-uri

Caracteristicile Bitdefender MDR

Cea mai bună platformă de securitate – Bitdefender MDR include platforma noastră de securitate de top la nivelul industriei, îmbunătățită cu instrumente SOC suplimentare și tehnologii AI

- **Protecție 24/7 –** Rețeaua noastră globală de centre de operațiuni de securitate (SOC) lucrează oricând lucrați și dumneavoastră și nu numai, oferindu-vă servicii de asistență oriunde v-ați afla și în orice moment. Dacă are loc un incident de securitate, echipa SOC va lua măsuri, iar administratorul de cont va suna persoana de contact în caz de urgență în termen de 30 de minute și va asigura o comunicare constantă pe toată durata incidentului.
- **Acțiuni pre-aprobate (PAA) –** Gama variată de acțiuni aprobate în prealabil (PAA) asigură un răspuns rapid și decisiv pentru a remedia incidentele de securitate. Analiștii noștri evaluează, investighează și iau măsuri mai rapid decât orice altă echipă.
- **Threat Hunting –** datorită numărului foarte mare de endpointuri protejate, cercetătorii în securitate de la Bitdefender și echipele Bitdefender Labs și MDR Threat Intelligence pot compila un volum uriaș de date de tip threat intelligence, informații despre atacatori și analize ale amenințărilor, pentru a le oferi clienților informații actualizate și pentru a-i sprijini în eforturile de threat hunting.
- **Recomandări de la experți –** Pe lângă faptul că asigurăm o securitate completă, vă ajutăm echipa de securitate să lucreze mai bine. Echipa noastră de experți în securitate vă oferă recomandări pentru a vă îmbunătăți cunoștințele și postura de securitate, precum și acțiuni corective pentru a preveni posibile incidente.
- **Analiza cauzei și impactului incidentului –** Identificăm vectorii inițiali ai amenințării și impactul potențial în timpul incidentelor, oferind analize complete și documentația aferentă în cadrul rapoartelor post-acțiune. Asigurăm o monitorizare sporită timp de 72 de ore pentru a ne asigura că nu se mai produc incidente similare sau conexe.
- **Portal MDR și funcționalități de raportare –** portalul MDR oferă dashboard-uri avansate și rapoarte lunare, care conțin informații practice cu privire la serviciul dumneavoastră. Rapoartele oferă informații utile despre incidentele de securitate, evidențiază tendințele în materie de securitate cibernetică și vă îndrumă în demersurile de remediere a problemelor, oferind o transparență inegalabilă la nivelul serviciului MDR.
- **Asigurare în cazul producerii unei breșe de securitate cibernetică:** Clienții MDR beneficiază de asigurare în valoare de până la 100.000 USD în cazul producerii unui incident de tip ransomware.

Caracteristicile Bitdefender MDR PLUS

Sunt incluse toate beneficiile pe care le oferă Bitdefender MDR

- **Administrator de cont disponibil 24x7 –** Administratorul de cont (SAM – Security Account Manager) dedicat este punctul dumneavoastră unic de contact, gata să vă răspundă la întrebări sau orice probleme care vă preocupă și să efectueze o analiză trimestrială (QBR).
- **Onboarding de servicii profesionale –** echipa de servicii profesionale oferă asistență și instrucțiuni detaliate pentru ca organizația dumneavoastră să integreze rapid serviciile oferite.
- **Fluxuri de threat intelligence și analiza globală a acestor date –** Cyber Intelligence Fusion Cell (CIFC) utilizează ciclul de viață al datelor de tip threat intelligence pentru a cerceta amenințările cibernetice, activitatea geopolitică și tendințele în materie de date specifice industriei și aplică aceste cunoștințe la nivelul organizației dumneavoastră.
- **Monitorizare pe Dark Web –** asigură o monitorizare continuă pe Dark Web, inclusiv pe forumuri și platforme comerciale populare în rândul grupărilor infracționale, precum și pe bloguri de ransomware, pentru a detecta date furate sau sustrase aparținând unor organizații, inclusiv domenii, date de autentificare, proprietate intelectuală (IP), trimiteri la brand și typo-squatting, stackul de tehnologii și preocupări generale referitoare la industrie și arii geografice.
- **Stabilirea cerințelor de bază în domeniul securității și crearea de modele adaptate ale amenințărilor –** adunăm și prelucrăm informații despre organizația dumneavoastră, inclusiv despre activitatea desfășurată, utilizatori și amenințări cunoscute, pentru a crea modele și a monitoriza peisajul amenințărilor specific companiei dumneavoastră.
- **Protecția mărcii și a proprietății intelectuale –** monitorizați-vă în mod continuu cele mai valoroase bunuri pentru ca noi să putem detecta și să vă putem notifica în legătură cu orice informații partajate sau vândute pe Dark Web care vă aparțin.
- **Monitorizarea țintelor de importanță majoră –** monitorizați în permanență angajații de importanță majoră pentru a depista eventualele informații care ar fi putut fi furate sau divulgate.
- **Rapoarte detaliate –** inclusiv date de threat hunting, Tippers (cercetări și recomandări specifice industriei) și Solicitări de informații (cerute de clienți)
- **Asigurare în cazul producerii unei breșe de securitate cibernetică:** Clienții MDR beneficiază de asigurare în valoare de până la 1.000.000 USD în cazul producerii unui incident de securitate.

Bitdefender MDR pentru MSP-uri

Bitdefender MDR pentru MSP le oferă clienților funcționalități solide de securitate, fără să fie nevoie de resurse interne extinse. Clienții furnizorilor de servicii administrate beneficiază de protecție continuă împotriva amenințărilor cibernetice actuale și emergente, eliminând o mare parte din eforturile MSP-urilor în materie de securitate. Acest lucru le permite acestora să își concentreze resursele pe dezvoltarea strategică a companiei, managementul relațiilor cu clienții și îmbunătățirea ofertelor de servicii de bază.

Beneficiile pentru furnizorii de servicii administrate

- **Creșterea veniturilor –** serviciul MDR oferă oportunități de creare a unor venituri suplimentare și de îmbunătățire a loialității clienților dumneavoastră.
- **Facturare automată –** oferă o experiență simplificată atât pentru MSP-uri, cât și pentru clienți.
- **Onboarding simplificat –** permite integrarea secvențială a mai multor clienți într-un proces simplu și repetabil.
- **Comunicații –** mijloacele multiple de comunicare și notificări sprijină interacțiunile la nivel de client.

Beneficiile pentru clienți

- **Protecție 24/7 –** Rețeaua noastră globală de centre de operațiuni de securitate (SOC) lucrează oricând lucrați și dumneavoastră, oferindu-vă servicii de asistență oriunde v-ați afla și în orice moment. Dacă are loc un incident de securitate, echipa SOC va lua măsuri, iar administratorul de cont va suna persoana de contact în caz de urgență în termen de 30 de minute.
- **Acțiuni pre-aprobate (PAA) –** O gamă variată de acțiuni aprobate în prealabil (PAA) asigură un răspuns rapid și

decisiv pentru a remedia incidentele de securitate. Analiștii noștri evaluează, investighează și iau măsuri mai rapid decât orice altă echipă.

- **Threat Hunting –** datorită numărului foarte mare de endpointuri acoperite, echipele Bitdefender pot compila un volum uriaș de date de tip threat intelligence, informații despre atacatori și analize ale amenințărilor, pentru a le oferi constant clienților dumneavoastră informații actualizate și pentru a-i sprijini în eforturile de threat hunting.
- **Portal MDR și funcționalități de raportare –** portalul MDR oferă dashboard-uri avansate și rapoarte lunare, care conțin informații practice cu privire la serviciul dumneavoastră pentru clienți.

Descrierea detaliată a serviciilor Bitdefender MDR

Monitorizare și asistență 24x7

Bitdefender MDR oferă un serviciu cuprinzător de securitate cibernetică, care operează 24x7, din trei centre de operațiuni de securitate (SOC), unul în America de Nord (SUA-Texas), unul în Europa (România) și unul în Asia Pacific (Singapore). Fiecare dintre SOC-urile noastre sunt dotate cu personal certificat de același nivel, procesele și tehnologiile necesare pentru a ne asigura că le oferim clienților noștri din întreaga lume acoperire neîntreruptă, disponibilă 24x7, 365 de zile pe an. Centrele noastre de operațiuni globale se asigură că clienții dintr-o anumită regiune sunt sprijiniți de un SOC din aceeași regiune în timpul programului lor de lucru.

La baza serviciului nostru MDR se află capacitatea de răspuns rapid. În cazul detectării unui incident de securitate, vom executa acțiuni pre-aprobate (vezi mai jos). Acest lucru îi permite serviciului nostru MDR să acționeze imediat, evitând eventual daune înainte ca acestea să apară și câștigând timp prețios pentru investigații și remedieri ulterioare.

Bitdefender MDR le oferă clienților recomandări detaliate de remediere, adaptate incidentului specific. Aceste recomandări pot presupune o varietate de măsuri, cum ar fi corectarea vulnerabilităților software, ajustarea setărilor de securitate, îmbunătățirea măsurilor de control al accesului utilizatorilor și/sau luarea de măsuri pentru anumite fișiere și procese. Această abordare cuprinzătoare nu numai că ajută la rezolvarea incidentului actual, dar contribuie și la consolidarea posturii generale de securitate a organizației împotriva amenințărilor viitoare.

Oferind monitorizare non-stop, răspuns instantaneu și îndrumări pentru remediere, Bitdefender MDR oferă o soluție completă pentru gestionarea și răspunsul la amenințările cibernetice, permițându-le organizațiilor să se concentreze asupra operațiunilor lor principale.

Acțiuni aprobate în prealabil

Răspunsurile pre-aprobate sau proactive la incidente reprezintă o capacitate cheie a echipei Bitdefender MDR. Analiștii noștri evaluează rapid incidentele de securitate și iau măsuri decisive pentru a limita și atenua amenințarea. Prin colaborare cu stakeholderi din cadrul organizației, aceștia oferă actualizări și îndrumări într-un mod regulat pe parcursul evenimentului de securitate. Investigațiile amănunțite ajută la identificarea cauzei principale a incidentului și la colectarea de informații, în timp ce eforturile de recuperare și remediere se concentrează pe restabilirea sistemelor afectate.

Echipa MDR menține constant comunicarea cu o listă pre-aprobată de contacte de urgență din cadrul organizației pe tot parcursul incidentului de securitate, oferind îndrumări și informându-i cu privire la orice acțiuni pre-aprobate întreprinse în conformitate cu acordul privind nivelul de servicii. Acțiunile pre-aprobate includ:

- **Întreruperea unui proces:** experții noștri vor opri un proces despre care au stabilit că este periculos.
- **Blocarea unui fișier:** experții noștri vor bloca executarea unui fișier periculos pe dispozitivul gazdă.
- **Excluderea unui fișier sigur:** experții noștri vor adăuga un fișier sigur la o listă de excepții pentru a preveni alarmele false.

- **Adăugarea unui fișier în Sandbox:** experții noștri vor încărca un fișier în Sandbox GravityZone pentru detonare și analiză.
- **Căutarea de informații despre fișiere:** experții noștri vor căuta informații despre fișiere disponibile pe VirusTotal și motoarele de căutare pentru a determina ce informații disponibile există deja.
- **Aplicarea patch-urilor:** în cazul în care clientul are add-onul GravityZone Patch Management, experții noștri vor aplica patch-urile pentru o aplicație care a fost identificată într-un incident ca având o vulnerabilitate.
- **Colectarea pachetului de investigare:** experții noștri vor colecta un pachet de investigare GravityZone de la endpointul respectiv pentru a efectua analize ulterioare.
- **Shell de răspuns:** experții noștri pot avea acces să execute comenzi pe endpointul relevant pentru a investiga sau a remedia activitățile periculoase.
- **Blocarea unui port:** experții noștri vor împiedica gazda să facă trafic în rețea pe unul sau mai multe porturi de rețea dacă acestea prezintă un risc. Cum ar fi portul 80 sau 443.
- **Blocarea unei adrese IP:** experții noștri vor bloca gazda să facă schimb de trafic de rețea cu una sau mai multe adrese IP despre care au constatat că sunt periculoase.
- **Izolarea unei gazde:** experții noștri vor deconecta gazda de la rețea, astfel încât să nu mai creeze sau să primească conexiuni cu alte sisteme.
- **Ștergerea unui fișier:** experții noștri vor șterge un fișier despre care au stabilit că este periculos.
- **Mutarea în carantină a unui fișier:** experții noștri vor muta un fișier suspect într-un director de carantină, astfel încât să nu poată fi folosit accidental. Fișierul nu va fi șters.
- **Dezactivarea unui cont de utilizator compromis:** experții noștri vor dezactiva contul unui utilizator compromis în Active Directory, Azure, Office 365 și AWS IAM.
- **Resetarea forțată a parolei pentru un cont de utilizator compromis:** experții noștri vor forța resetarea parolei pentru un cont de utilizator compromis în Active Directory, Azure și Office 365.
- **Marcarea unui cont de utilizator ca fiind compromis:** experții noștri vor marca orice cont identificat ca fiind compromis într-un incident ca atare.
- **Ștergerea unui e-mail periculos:** experții noștri vor șterge un e-mail identificat ca fiind periculos într-un incident în Exchange Online/Office 365.

Threat Hunting

Bitdefender monitorizează, compilează și analizează o cantitate uriașă de informații despre amenințări, cercetări asupra atacatorilor și date de la endpointuri și de la senzori pentru a actualiza continuu peisajul amenințărilor, a sprijini activitatea de threat hunting și a proteja mediile clienților noștri.

Înțelegând tacticile, tehnicile și procedurile (TTP) folosite de potențialii atacatori, putem anticipa și detecta mai bine amenințările.

Tehnicile avansate de analiză și de detecție a amenințărilor sunt apoi aplicate pentru a analiza aceste date, căutând modele, anomalii, indicatori de compromitere (IOC), exploit-uri zero-day și amenințări interne care prezintă riscuri semnificative pentru organizație. Apoi, comparăm datele cu semnăturile de atac cunoscute și cu valori de referință comportamentale pentru a identifica activități suspecte care ar putea indica o potențială amenințare sau un atac în curs.

Amenințările detectate sunt apoi triate și ierarhizate în funcție de gravitatea lor și de impactul potențial asupra organizației dumneavoastră. Această ierarhizare le permite analiștilor să-și concentreze resursele și atenția mai întâi asupra celor mai critice amenințări, asigurând eforturi eficiente de răspuns și remediere. Investigațiile sunt efectuate pentru a culege informații suplimentare și pentru a determina natura și amploarea amenințărilor. Echipa Bitdefender MDR ia măsurile adecvate pentru a atenua efectele amenințărilor, cum ar fi izolarea sistemelor afectate, blocarea traficului periculos sau inițierea procedurilor de răspuns la incidente.

Pe parcursul întregului proces, punem accent pe monitorizarea și îmbunătățirea continuă. Evaluăm continuu situația de securitate a organizației dumneavoastră, analizăm noile amenințări și perfecționăm capacitățile de detecție și răspuns la acestea. Fiecare incident devine o oportunitate de învățare pentru a vă consolida întreaga apărare în domeniul

securității cibernetice. În plus, oferim actualizări regulate, rapoarte despre incidente și recomandări, pentru a fi mereu la curent și pentru a vă implica activ în procesul de threat hunting.

Funcționalități complete de raportare și vizibilitate

Bitdefender recunoaște importanța serviciilor sale MDR pentru a comunica detalii complexe și informații privind serviciile pe care le oferim clienților noștri. În acest scop, în serviciile noastre MDR am integrat funcționalități complete de raportare, cu informații practice. Aceste rapoarte se bazează pe analize de volume mari de date, inteligență artificială și expertiză umană. Rapoartele oferă informații utile despre incidentele de securitate, evidențiază tendințele în materie de securitate cibernetică și vă îndrumă în demersurile de remediere a problemelor, oferind o transparență inegalabilă la nivelul serviciului MDR.

Capacitățile noastre de raportare facilitează conformitatea cu reglementările, ajută la identificarea și atenuarea vulnerabilităților și oferă o platformă pentru îmbunătățirea continuă a securității. Servind ca instrument de comunicare indispensabil între părțile interesate, rapoartele noastre permit luarea deciziilor în cunoștință de cauză și planificarea strategică.

În secțiunea următoare, vom prezenta diferitele tipuri de rapoarte oferite de serviciul Bitdefender MDR. Rapoartele sunt accesibile prin Portalul Bitdefender MDR.

Raport lunar

Raportul nostru lunar MDR oferă o imagine detaliată a peisajului dumneavoastră de securitate. Acesta include o analiză cuprinzătoare a activității de bază la nivelul gazdelor și rețelei, precum și dinamica mediului și a utilizatorilor în ultima

lună. Raportul începe cu o prezentare generală a activităților generale, cum ar fi activitatea agenților și a rețelei, alertele EDR și amenințările descoperite. Apoi, detaliază aceste informații oferind un context esențial pentru înțelegerea posturii de securitate cibernetică a organizației dumneavoastră.

Secțiunea de gestionare a cazurilor oferă o imagine de ansamblu detaliată a tuturor cazurilor de securitate în curs și închise, evidențiind natura amenințărilor și măsurile luate pentru remediere. Raportul se încheie cu o analiză amănunțită a activității lunare de securitate care prezintă statistici esențiale privind detecția amenințărilor, activitatea de threat hunting, alertele aferente activității de intelligence și activitățile de caz. Raportul lunar este un instrument esențial pentru a asigura un management coerent și proactiv al securității.

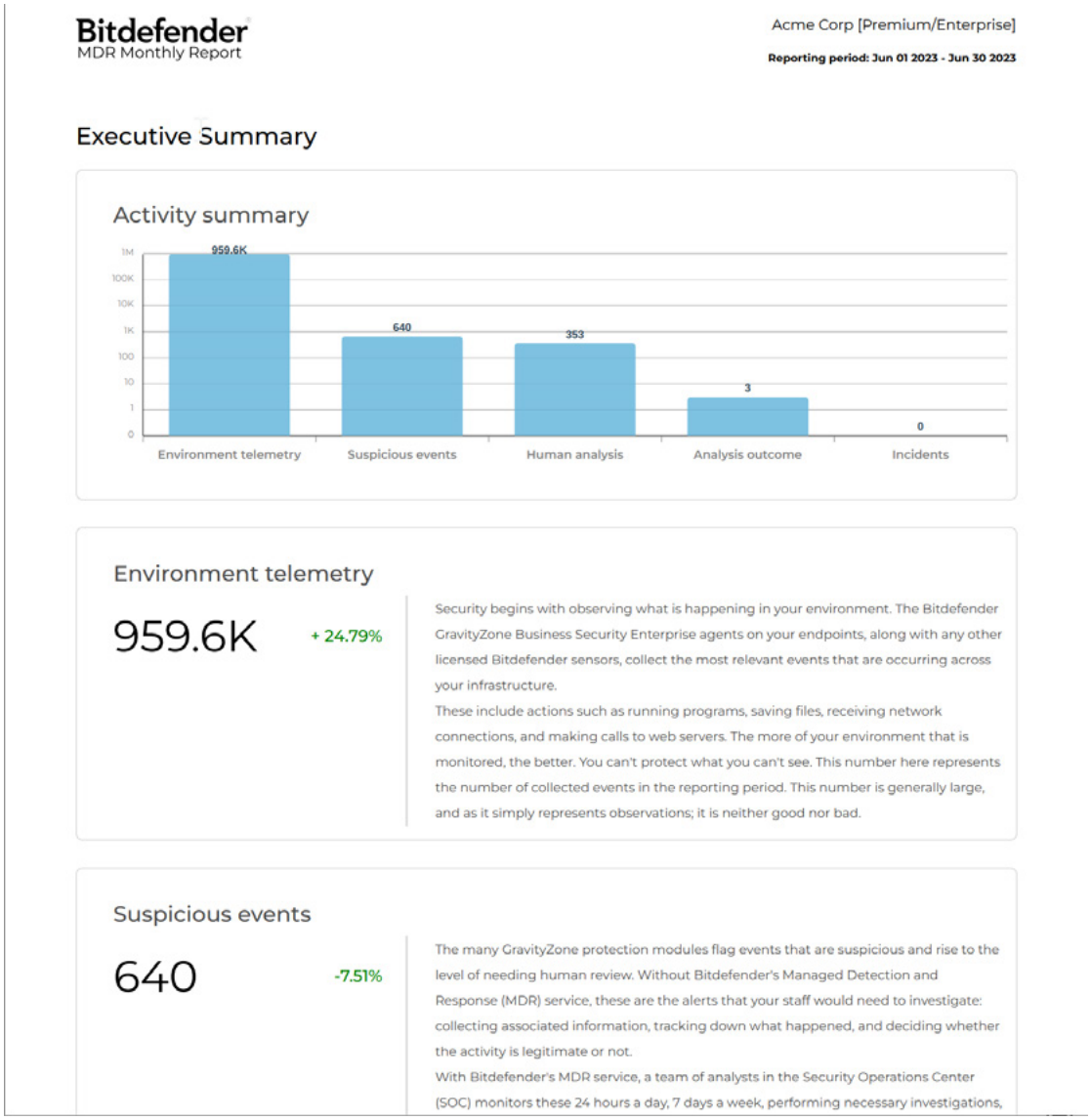


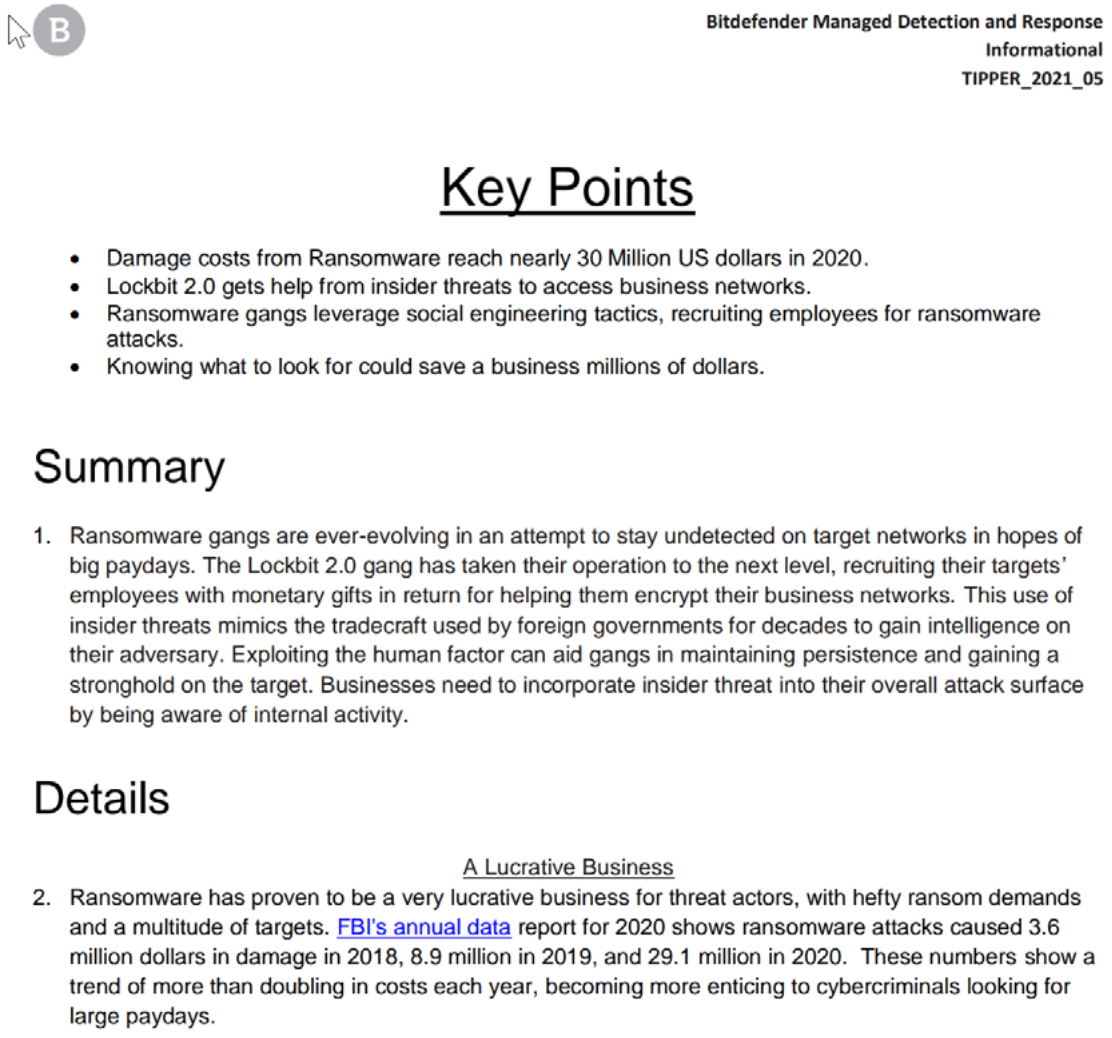
Figura 1: Un exemplu de secțiune a Raportului lunar Bitdefender MDR.

Raportul Tipper

Raportul Tipper Bitdefender MDR este un instrument de informații crucial, conceput special pentru a oferi informații actualizate despre anumiți atacatori, tendințele emergente din domeniul securității cibernetice sau informații despre sectorul de activitate al clientului și despre modul în care acesta este vizat de atacatori. Bazate pe o colecție cuprinzătoare de informații despre amenințări, aceste rapoarte acționează ca un sistem de avertizare timpurie privind atacurile cibernetice potențial dăunătoare, permițându-le organizațiilor să fie mereu cu un pas înainte în peisajul amenințărilor care continuă să evolueze. Rapoartele Tipper sunt generate printr-o combinație de AI și expertiză

umană de către echipa noastră Cyber Intelligence Fusion Cell (CIFC). Informațiile sunt colectate din fluxurile globale de securitate cibernetică, activitățile de pe Dark Web, precum și din tendințele și modelele derivate din datele organizației dumneavoastră.

Fiecare raport Tipper este format din patru secțiuni principale. „Rezumatul" oferă o imagine de ansamblu la nivel înalt a amenințării sau tendinței identificate, sub forma unei prezentări succinte a impactului potențial și a domeniilor afectate. Secțiunea „Detalii" analizează elementele specifice, inclusiv modul de operare al atacatorului sau atributele tehnice ale unei anumite amenințări sau tendințe cibernetice. Această secțiune ajută organizațiile să înțeleagă natura problemei în cauză. Secțiunea „Recomandări" oferă informații utile despre cum să atenuați efectele sau să vă protejați împotriva amenințării identificate, adaptate la mediul tehnic al organizației dumneavoastră. Aceasta ar putea include recomandări privind patch-urile, modificări ale configurației sistemului sau o mai bună monitorizare a anumitor activități. Nu în ultimul rând, secțiunea „Referințe" oferă resurse care conțin informații sau îndrumări suplimentare, cum ar fi buletine de la agențiile de securitate cibernetică, lucrări sau link-uri către cercetări relevante din industrie. Aceste componente se reunesc pentru a crea un raport care oferă o imagine cuprinzătoare și concretă a peisajului amenințărilor.



Bitdefender Managed Detection and Response
Informational
TIPPER_2021_05

Key Points

- Damage costs from Ransomware reach nearly 30 Million US dollars in 2020.
- Lockbit 2.0 gets help from insider threats to access business networks.
- Ransomware gangs leverage social engineering tactics, recruiting employees for ransomware attacks.
- Knowing what to look for could save a business millions of dollars.

Summary

1. Ransomware gangs are ever-evolving in an attempt to stay undetected on target networks in hopes of big paydays. The Lockbit 2.0 gang has taken their operation to the next level, recruiting their targets' employees with monetary gifts in return for helping them encrypt their business networks. This use of insider threats mimics the tradecraft used by foreign governments for decades to gain intelligence on their adversary. Exploiting the human factor can aid gangs in maintaining persistence and gaining a stronghold on the target. Businesses need to incorporate insider threat into their overall attack surface by being aware of internal activity.

Details

A Lucrative Business

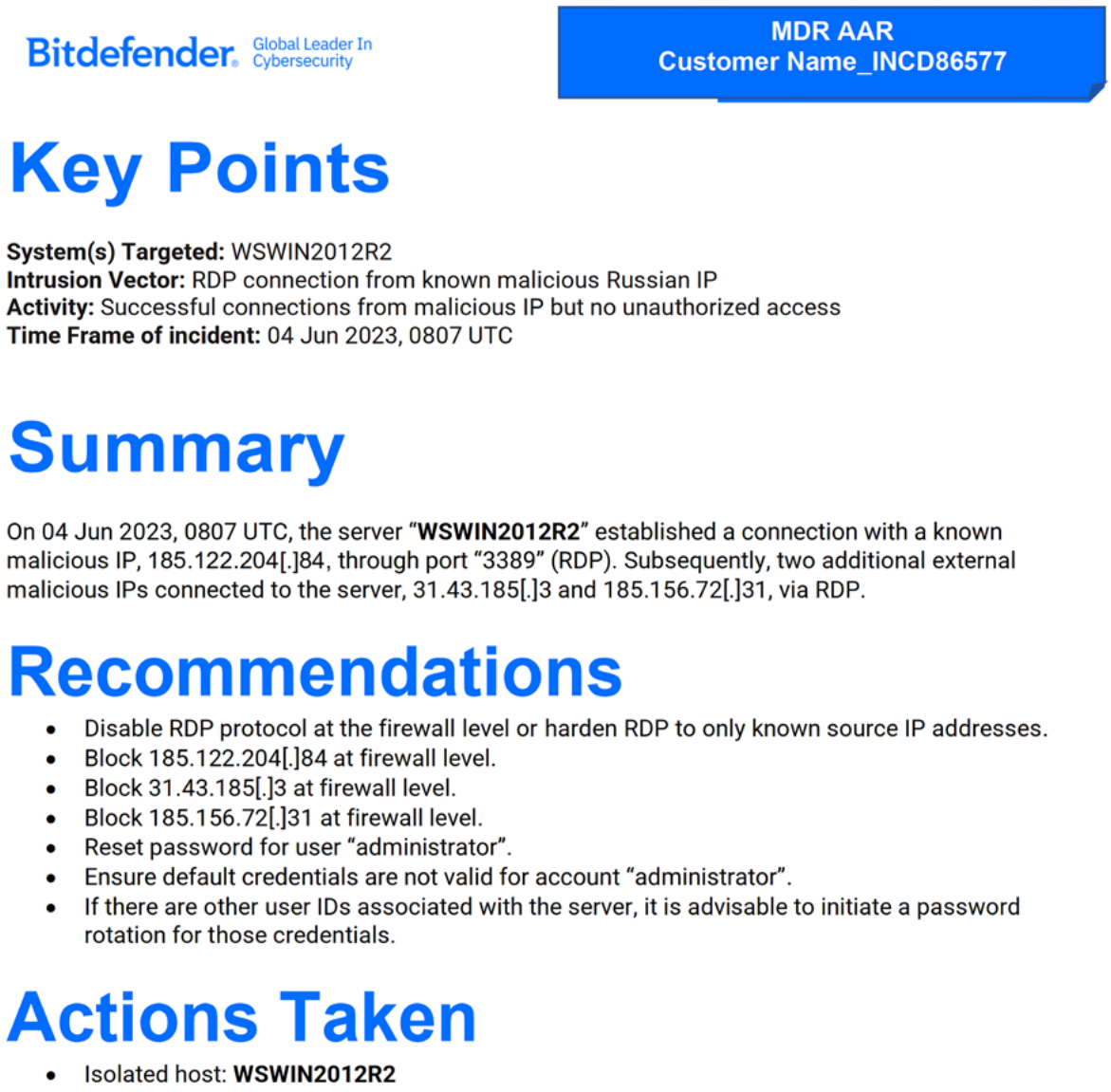
2. Ransomware has proven to be a very lucrative business for threat actors, with hefty ransom demands and a multitude of targets. FBI's annual data report for 2020 shows ransomware attacks caused 3.6 million dollars in damage in 2018, 8.9 million in 2019, and 29.1 million in 2020. These numbers show a trend of more than doubling in costs each year, becoming more enticing to cybercriminals looking for large paydays.

Figura 2: Un exemplu de secțiune din Raportul Tipper Bitdefender MDR

Raportul rapid

Când este detectat pentru prima dată un incident de securitate, este important să anunțați organizația despre ceea ce știe echipa MDR înainte de finalizarea investigației. Aici intervine raportul rapid. Acest raport este o metodă folosită pentru a comunica informații concise privind activitățile suspecte detectate în mediul clientului. Include puncte cheie,

care evidențiază sistemele afectate inițial, cronologia incidentului, un rezumat al elementelor detectate și acțiunile întreprinse de echipa de securitate Bitdefender. Odată ce investigația este finalizată, clientului i se oferă rapoartele post-acțiune menționate mai sus, care oferă mai multe detalii.


Bitdefender Global Leader In Cybersecurity

MDR AAR
Customer Name_INCD86577

Key Points

System(s) Targeted: WSWIN2012R2
Intrusion Vector: RDP connection from known malicious Russian IP
Activity: Successful connections from malicious IP but no unauthorized access
Time Frame of incident: 04 Jun 2023, 0807 UTC

Summary

On 04 Jun 2023, 0807 UTC, the server "**WSWIN2012R2**" established a connection with a known malicious IP, 185.122.204[.]84, through port "3389" (RDP). Subsequently, two additional external malicious IPs connected to the server, 31.43.185[.]3 and 185.156.72[.]31, via RDP.

Recommendations

- Disable RDP protocol at the firewall level or harden RDP to only known source IP addresses.
- Block 185.122.204[.]84 at firewall level.
- Block 31.43.185[.]3 at firewall level.
- Block 185.156.72[.]31 at firewall level.
- Reset password for user "administrator".
- Ensure default credentials are not valid for account "administrator".
- If there are other user IDs associated with the server, it is advisable to initiate a password rotation for those credentials.

Actions Taken

- Isolated host: **WSWIN2012R2**

Figura 3: Un exemplu de secțiune a Raportului rapid Bitdefender MDR

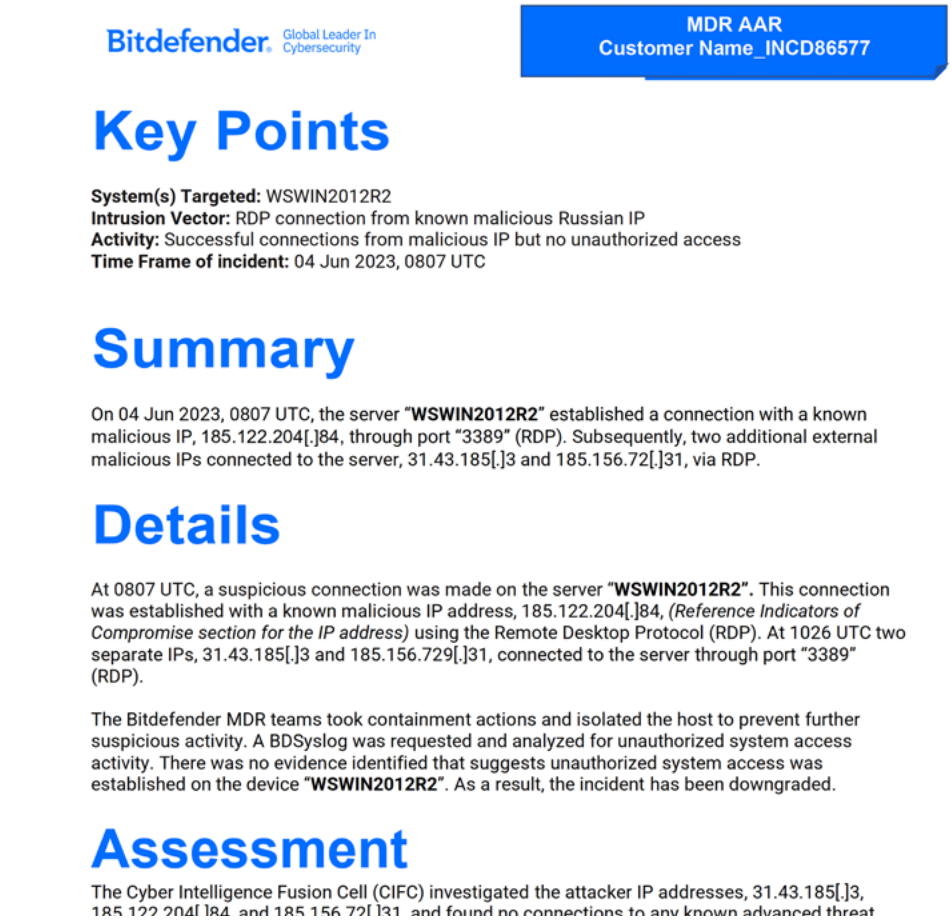
Raportul post-acțiune

Raportul post-acțiune este un document complet, care oferă o analiză cuprinzătoare a unui incident de securitate cibernetică care a avut loc în mediul unui client. Acest raport este esențial pentru înțelegerea ciclului de viață complet al unei tentative de breșă de securitate a datelor, începând de la apariția acesteia până la eventuala izolare și remediere a breșei. Raportul detaliază gravitatea incidentului, oferind un rezumat a ceea ce s-a întâmplat, vectorii de intruziune, descrierea generală a mediului, rezumatul analiștilor și detaliile incidentului și acțiunile întreprinse de echipa Bitdefender MDR pentru a remedia amenințarea.

Raportul detaliază succesiunea precisă a evenimentelor care au avut loc în timpul tentativei de breșă. Acesta include detecția inițială, acțiunile ulterioare întreprinse, procesul de răspuns și recuperare a datelor, fișierele, rețelele și sistemele implicate în atac. Raportul prezintă acțiunile specifice întreprinse pentru identificarea, limitarea și eliminarea amenințării. Aici sunt incluși pași precum izolarea sistemelor infectate, aplicarea de patch-uri pentru vulnerabilitățile descoperite, eliminarea programelor malware și orice alte măsuri luate pentru a neutraliza amenințarea și a minimiza impactul acesteia.

Furnizat după o perioadă de 72 de ore de monitorizare post-incident de înaltă prioritate, raportul se încheie cu o listă aprofundată de recomandări pentru a preveni astfel de incidente în viitor. Aceste sugestii ar putea varia de la consolidarea controalelor de securitate și îmbunătățirea procedurilor de răspuns la incidente, până la programe de instruire și informare ale angajaților.

Oferind o relatare amănunțită a incidentului și pași practici de prevenție în viitor, un raport „post-acțiune” servește ca instrument de învățare, ajutând organizațiile să-și îmbunătățească postura de securitate cibernetică și reziliența la atacurile viitoare.



Bitdefender Global Leader In Cybersecurity

MDR AAR
Customer Name_INCD86577

Key Points

System(s) Targeted: WSWIN2012R2
Intrusion Vector: RDP connection from known malicious Russian IP
Activity: Successful connections from malicious IP but no unauthorized access
Time Frame of incident: 04 Jun 2023, 0807 UTC

Summary

On 04 Jun 2023, 0807 UTC, the server **"WSWIN2012R2"** established a connection with a known malicious IP, 185.122.204[.]84, through port "3389" (RDP). Subsequently, two additional external malicious IPs connected to the server, 31.43.185[.]3 and 185.156.72[.]31, via RDP.

Details

At 0807 UTC, a suspicious connection was made on the server **"WSWIN2012R2".** This connection was established with a known malicious IP address, 185.122.204[.]84, *(Reference Indicators of Compromise section for the IP address)* using the Remote Desktop Protocol (RDP). At 1026 UTC two separate IPs, 31.43.185[.]3 and 185.156.729[.]31, connected to the server through port "3389" (RDP).

The Bitdefender MDR teams took containment actions and isolated the host to prevent further suspicious activity. A BDSyslog was requested and analyzed for unauthorized system access activity. There was no evidence identified that suggests unauthorized system access was established on the device **"WSWIN2012R2"**. As a result, the incident has been downgraded.

Assessment

The Cyber Intelligence Fusion Cell (CIFC) investigated the attacker IP addresses, 31.43.185[.]3, 185.122.204[.]84, and 185.156.72[.]31, and found no connections to any known advanced threat

Figura 4: Un exemplu de secțiune din Raportul post-acțiune Bitdefender MDR

Analiza cauzei și impactului incidentului

Identificăm vectorii inițiali ai amenințării și impactul potențial în timpul incidentelor, oferind analize complete și documentația aferentă în cadrul rapoartelor post-acțiune. Asigurăm o monitorizare sporită timp de 72 de ore pentru a ne asigura că nu se mai produc incidente similare sau conexe.

Recomandări de la experți

Pe lângă faptul că asigurăm o securitate completă, vă ajutăm echipa de securitate să lucreze mai bine. Echipa noastră de experți în securitate vă oferă recomandări pentru a vă îmbunătăți cunoștințele și postura de securitate, precum și acțiuni corective pentru a preveni posibile incidente.

Servicii specifice Bitdefender MDR PLUS

Manager de cont de securitate dedicat

Administratorul de cont de securitate (SAM – Security Account Manager) dedicat este singurul dumneavoastră punct de contact cu Bitdefender. SAM vă stă la dispoziție pentru a vă răspunde la întrebări și pentru a vă oferi o evaluare trimestrială a activității (QBR – Quarterly Business Review) pentru a comunica în mod clar starea securității companiei dumneavoastră, problemele nerezolvate și recomandările aferente. Dacă are loc un incident de securitate, echipa SOC va lua măsuri, iar SAM va suna persoana de contact în caz de urgență în termen de 30 de minute și va asigura o comunicare constantă pe toată durata incidentului.

Modele adaptate ale amenințărilor

Începând de la onboarding și perioada inițială de dezvoltare a unui nivel de referință al securității, colectăm și prelucrăm în mod continuu informații despre organizația dumneavoastră, inclusiv despre activitatea desfășurată, utilizatori și amenințări cunoscute, pentru a crea modele și a monitoriza peisajul amenințărilor specific companiei dumneavoastră.

O componentă de bază a modelelor adaptate ale amenințărilor este crearea unui context suplimentar și cuprinzător al mediului unic al clientului, care este mai întâi pus laolaltă sub forma unui Chestionar detaliat pentru clienți, din care aflăm despre domenii, utilizatori cheie care ar putea fi vizați într-o campanie de phishing, informații despre brand, sectoare industriale, zone geografice în care își desfășoară activitatea clienții noștri și multe altele. Acest chestionar inițial ne ajută să ne adaptăm serviciile fiecărui client în parte și ne permite să abordăm riscurile și nevoile specifice de securitate ale acestora.

Bitdefender MDR stabilește apoi valori de bază în domeniul securității pentru clienții noștri. Acest lucru le oferă organizațiilor mai multe beneficii cheie. În primul rând, permite o evaluare cuprinzătoare a riscurilor și identifică lacunele în postura de securitate a organizației, permițând alocarea eficientă a resurselor și ierarhizarea acestora. Astfel, organizația va putea înțelege peisajul actual al riscurilor și va alinia măsurile de securitate în consecință.

În al doilea rând, stabilirea valorilor de bază în domeniul securității îmbunătățește capacitățile de detecție și răspuns la incidente. Prin stabilirea unui punct de referință pentru activitățile și comportamentele normale din cadrul infrastructurii IT a organizației, abaterile de la valori de bază declanșează alerte, permițând un răspuns rapid și investigarea potențialelor amenințări. Această abordare proactivă minimizează timpul necesar pentru identificarea și eliminarea incidentelor de securitate, reducând daunele potențiale și permițând un răspuns rapid.

Stabilirea unor valori de bază îi permite echipei noastre MDR să creeze un model unic de amenințare pentru fiecare client. Crearea de modele ale amenințărilor constituie un element esențial în stabilirea valorilor de referință și asigură dezvoltarea și menținerea unei înțelegeri precise a peisajului amenințărilor pentru mediul monitorizat.

Procesul de creare a modelelor de amenințări începe cu stabilirea cerințelor de intelligence care să vină în sprijinul obiectivelor strategice ale companiei, pentru a face față ritmului dinamic al peisajului amenințărilor cibernetice și noilor amenințări observate. Cercetarea continuă le oferă clienților informații detaliate despre cine, ce, unde și de ce atacatorii cibernetici le-ar putea viza compania. Pe baza detaliilor colectate din Chestionarul pentru clienți, se creează un model al amenințărilor în platformele Security Orchestration, Automation, & Response Platform (SOAR) și Threat Intelligence Platform (TIP). Modelul cuprinde un rezumat al contextului, care include tendințele din industrie, incidentele recente și conexe și vectorii cheie de atac care trebuie monitorizați.

Cercetarea efectuată și informațiile obținute vor susține activitatea de threat hunting și rapoartele de consiliere trimise clientului, ambele putând furniza:

- constatări specifice privind riscurile și amenințările;
- cunoașterea contextului;
- recomandări de atenuare a efectelor.

Această abordare îmbunătățește acuratețea și eficiența detectării amenințărilor, asigurând o protecție proactivă și un răspuns eficient la incidentele de securitate.

Analiza globală a informațiilor

Analiștii noștri sunt organizați într-o structură denumită Cyber Intelligence Fusion Cell (CIFC), care utilizează ciclul de viață al datelor de tip threat intelligence pentru a cerceta amenințările cibernetice, activitatea geopolitică și tendințele în materie de date specifice industriei și aplică aceste cunoștințe la nivelul organizației dumneavoastră. Spre deosebire de alți furnizori, care pot încorpora o singură sursă externă de informații într-un serviciu de tip add-on, Bitdefender integrează în serviciul de bază mai multe surse, inclusiv pe cele proprii.

Monitorizare pentru Dark Web

Analiștii noștri monitorizează în permanență Dark Web-ul pentru a identifica surse cheie de informații precum forumuri, platforme și bloguri despre ransomware în vederea detectării datelor furate sau sustrase ce aparțin unor organizații, inclusiv domenii, date de autentificare, proprietate intelectuală (IP), referințe despre brand și typo-squatting, stackul de tehnologii și preocupări generale referitoare la industrie și arii geografice. De asemenea, putem monitoriza principalii furnizori și parteneri strategici pentru a vă notifica cu privire la eventualele problemele pe care le identificăm.

Protecția mărcii și IP-ului

Atunci când monitorizează Dark Web-ul, analiștii noștri caută mereu informații despre organizația dumneavoastră, despre brandul dumneavoastră și proprietatea intelectuală. Acestea sunt printre cele mai valoroase bunuri ale dumneavoastră. De aceea, pentru a le proteja, este esențial să detectăm ce anume se distribuie sau se vinde pe Dark Web. De asemenea, monitorizăm înregistrările de domenii pentru a detecta domeniile nou create care ar putea indica un comportament al atacatorilor de tip typo-squatting sau URL-hijacking. Pe lângă activitățile periculoase de pe internet, echipa mai monitorizează și informațiile sensibile expuse, cum ar fi parolele sau cheile de acces din depozitele de coduri.

Monitorizarea țintelor de importanță majoră

Nu este un secret faptul că persoanele din conducere și consiliile de administrație au acces la date foarte sensibile, dar nu respectă neapărat politicile și procedurile de securitate. Analiștii noștri pot monitoriza angajații de importanță majoră pentru a depista eventualele informații care ar fi putut fi furate sau divulgate.

Procesul de instalare și onboarding

Un proces de implementare și integrare fără probleme este esențial atunci când interacționați cu un furnizor de servicii MDR. Acest proces stabilește tonul pentru relația în desfășurare și poate influența semnificativ eficiența și eficacitatea serviciului MDR. Un plan de onboarding bine structurat se asigură că serviciul este integrat perfect în mediul IT existent, reducând la minimum întreruperile operațiunilor organizației.

Cu Bitdefender MDR, clienții au parte de un proces de onboarding transparent și cuprinzător, care încurajează încrederea și comunicarea între organizație și echipa de operațiuni de securitate Bitdefender, punând bazele unui parteneriat de succes, pe termen lung. În secțiunea următoare, vom descrie în detaliu procesul nostru de integrare și la ce se pot aștepta clienții.

Bitdefender MDR folosește produsul Bitdefender GravityZone Business Security Enterprise ca bază pentru tehnologia noastră de detecție a amenințărilor. Toți clienții MDR ar trebui să înceapă prin a-și crea contul GravityZone. Clienții pot utiliza Serviciile profesionale Bitdefender pentru companii pentru a-i ajuta la instalarea MDR. Serviciile profesionale sunt incluse în Bitdefender MDR PLUS. Clienții de bază Bitdefender MDR pot alege să adauge Servicii profesionale pentru a economisi timp și pentru a se asigura că toate configurațiile necesare sunt corecte.

Dacă clientul alege să folosească serviciile profesionale, va primi un e-mail de la echipa de servicii profesionale în termen de 2 zile lucrătoare de la cumpărare, cu informații despre cum să înceapă utilizarea.

Procesul de furnizare a serviciilor profesionale pentru companii

Furnizarea serviciilor profesionale pentru companii constă in cinci sesiuni:

↳ Apelul de inițiere

- ↳ Cunoașterea clientului
- ↳ Discuție despre nevoi și așteptări
- ↳ Evaluarea infrastructurii cu accent pe:
  - → Numărul de locații
  - → Numărul de endpointuri per locație
  - → Numărul de servere virtuale per locație/centru de date
  - → Tehnologia de virtualizare
  - → Furnizorul de securitate anterior
- ↳ Furnizarea de informații despre relee și servere de securitate
- ↳ Discutarea specificațiilor (SOW)
  - → Informarea clientului despre SOW
  - → Explicarea secțiunilor care trebuie completate
- ↳ Furnizarea planului de implementare:
  - → Configurarea GravityZone (2-4 ore)
  - → Inițierea procesului de instalare și validare (1-2 ore)
  - → Finalizarea instalării și verificarea instalărilor nereușite (2-3 ore)
  - → Verificarea bunei funcționări a produsului și acceptanța (1-2 ore)
- ↳ Stabilirea cerințelor hardware, software și de conectivitate
  - → Nu uitați să evidențiați ingestors-eu.bmdr.bitdefender.com și ingestors-us.bmdr.bitdefender.com pentru traficul MDR care trebuie trimis
- ↳ Furnizarea documentației GravityZone

↳ Sesiune de configurare GravityZone

În timpul configurării inițiale a GravityZone, trebuie să aplicați următorii pași:

- ↳ Configurarea consolei în cloud:
- ↳ Crearea contului GravityZone în cloud
- ↳ Crearea pachetelor de instalare (asigurați-vă că activați senzorul EDR în toate pachetele create)
- ↳ Crearea politicilor de securitate
  - → Nu configurați serverul Splunk în fila Security Telemetry
- ↳ Asigurați-vă că activați Senzorul EDR în toate politicile
  - → Creați integrări
  - → Creați reguli de atribuire și aplicați politici pe OU Active Directory, dacă este necesar
  - → Creați utilizatori
  - → Creați rapoarte
  - → Configurați notificări
  - → Creați o regulă de cleanup pentru mașinile offline
- ↳ Instalarea de relee și servere de securitate
- ↳ Tutorial GravityZone
  - → Explicați caracteristicile GravityZone

- Explicați cele mai bune practici de securitate
- Oferiți sfaturi pentru excepții
- Oferiți sfaturi privind întreținerea

Sesiunea de inițiere a procesului de instalare și validare

- Instalarea unui set de endpointuri pentru testare
- Atribuirea unei politici de securitate pentru acestea
- Verificarea endpointurilor pentru a identifica eventualele probleme
  - Verificați comunicarea
  - Verificați gradul de actualizare
  - Verificați conectivitatea serviciilor cloud
  - Telemetrie MDR (Verificați dacă starea telemetriei de securitate este stabilită și tipul de transport este Bitdefender MDR)
- Solicitați-i clientului să testeze și să valideze faptul că BEST nu interferează cu software-ul instalat

Sesiunea de finalizare a instalării și verificare a instalărilor nereușite

- Verificați endpointurile cu probleme
- Verificați instalările nereușite și efectuați remedierea erorilor inițiale
- Creați tichete de asistență pentru problemele descoperite

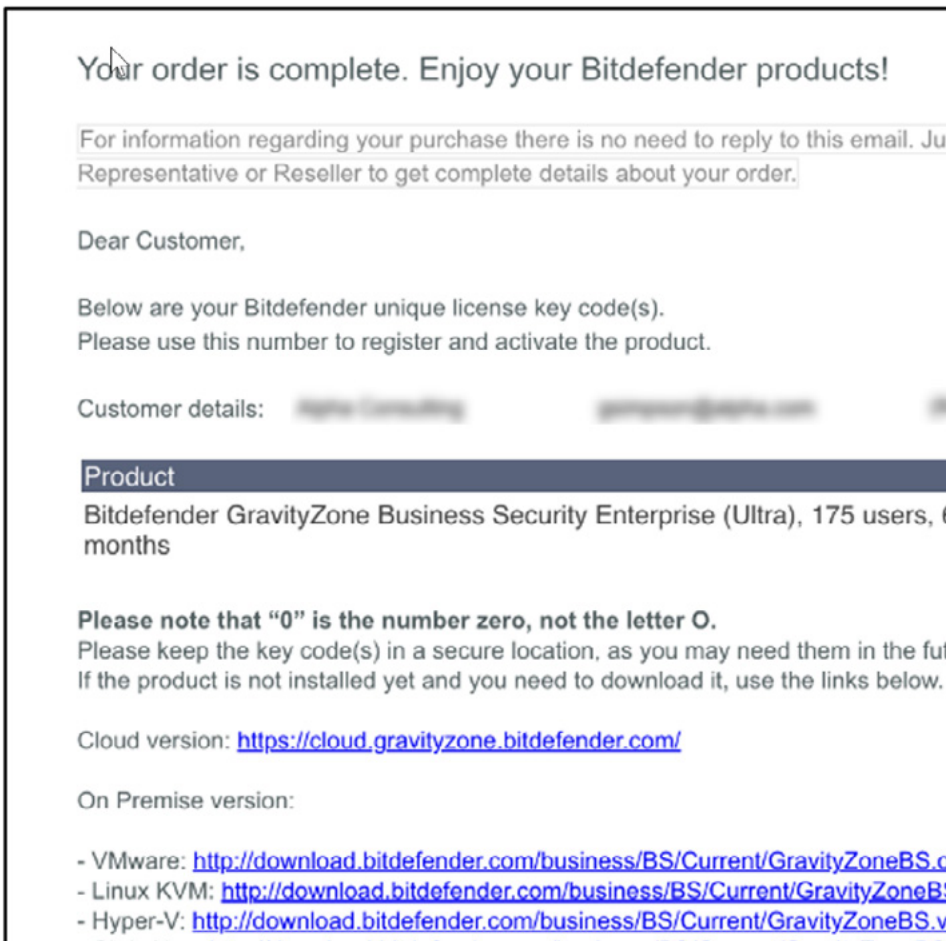
Sesiunea de verificare a bunei funcționări a produsului și de acceptare

- Verificarea endpointurilor
  - Actualizarea stării
  - Probleme de conectivitate
  - Probleme de performanță
- Verificarea releelor și a SVA-urilor pentru a identifica eventualele probleme de actualizare și conectivitate
- Examinarea politicilor și căutarea excepțiilor incorecte
- Verificarea stării modulului la nivelul endpointurilor
  - Validați dacă toate endpointurile au modulul EDR instalat și pornit
  - Verificați ce alte module sunt instalate
- Discuții despre procesul verbal de acceptanță
- Creați un poză a mediului clientului conform procedurii noastre de confluență și trimiteți-l echipei Customer Success Team (CST)

Odată ce acești pași sunt finalizați, furnizarea serviciilor profesionale MDR pentru companii este încheiată.

Crearea contului GravityZone și accesarea consolei GravityZone 18

Următorul pas în procesul de integrare este să vă conectați la consola Bitdefender GravityZone. Partenerul dvs. ar trebui să vă furnizeze o cheie de licență și datele de conectare pentru a vă conecta la consola GravityZone. În caz contrar, este posibil să fi primit un e-mail de la noreply-partnerlink@info.bitdefender.com ca acesta.


Your order is complete. Enjoy your Bitdefender products!

For information regarding your purchase there is no need to reply to this email. Ju
Representative or Reseller to get complete details about your order.

Dear Customer,

Below are your Bitdefender unique license key code(s).
Please use this number to register and activate the product.

Customer details:

Product

Bitdefender GravityZone Business Security Enterprise (Ultra), 175 users,
months

Please note that "0" is the number zero, not the letter O.
Please keep the key code(s) in a secure location, as you may need them in the fu
If the product is not installed yet and you need to download it, use the links below.

Cloud version: https://cloud.gravityzone.bitdefender.com/

On Premise version:

- VMware: http://download.bitdefender.com/business/BS/Current/GravityZoneBS.
- Linux KVM: http://download.bitdefender.com/business/BS/Current/GravityZoneB
- Hyper-V: http://download.bitdefender.com/business/BS/Current/GravityZoneBS.v

Figura 5: După ce v-ați creat contul GravityZone, căutați o scrisoare de bun venit ca aceasta.

Dacă ați primit doar un cod de produs, dar niciun fel de date de autentificare, vă puteți configura contul în GravityZone urmând acești pași.

Asistență post-onboarding

Odată ce clienții au finalizat procesul de integrare, dacă au nevoie de asistență din partea echipei MDR, îi încurajăm pe clienții Bitdefender MDR PLUS să contacteze managerul de cont care le-a fost alocat. Clienții Bitdefender MDR pot deschide un caz de asistență din Portalul pentru clienți MDR sau ne pot contacta prin unul dintre canalele de asistență descrise mai jos în acest document.

Cronologia instalării

Instalarea tehnologiei Bitdefender GravityZone poate fi realizată cu ușurință de partener sau client, folosind consola GravityZone, sau aceștia pot achiziționa serviciile echipei noastre Bitdefender Enterprise Professional Services. Detaliile instalării prin intermediul serviciilor profesionale pentru companii se regăsesc mai jos. Înainte de instalare, clientul trebuie să efectueze mai întâi pașii de onboarding descriși aici.

Pașii de onboarding

Odată ce clientul primește acces la portalul Bitdefender MDR, acesta se poate conecta și poate începe utilizarea. Pentru clienții MDR PLUS, procesul de onboarding se face prin completarea chestionarului nostru de onboarding. Chestionarul ne oferă un punct de plecare inițial pentru a construi o linie de referință pentru clienții noștri prin stabilirea de puncte de

date precise. Iată câteva dintre punctele de date specifice pe care le avem în vedere:

- Informații despre utilizatorii corporativi de la nivel executiv (de exemplu, utilizatorii cu rol de conducere), inclusiv nume, e-mailuri, nume de utilizator, nume de gazdă pentru stațiile lor de lucru, locațiile fizice din care lucrează în principal
- Sectoarele în care operează organizația
- Utilizatori care au drepturi superioare de acces la sisteme, cum ar fi administratorii de sistem
- Tipul de produse și/sau servicii oferite de organizație, inclusiv tipurile de date sensibile și clasificate pe care le stochează
- Furnizori terți care au acces la date sensibile
- Adrese IP și nume de domenii ale infrastructurii publice
- O hartă a rețelei

De ce să alegeți serviciul nostru MDR?

Există multe motive pentru care organizațiile ar trebui să aleagă Bitdefender MDR ca furnizor de soluții de securitate cibernetică, dintre care multe sunt deja evidențiate în acest document, însă cel mai important este calitatea echipei MDR, care este formată din analiști de securitate, experți în threat intelligence și în operațiuni. Următoarea secțiune prezintă aspectele prin care se remarcă echipa noastră MDR.

Experiența și expertiza noastră

Când vine vorba de securitate cibernetică, experiența contează, iar echipa noastră de operațiuni Managed Detection & Response (MDR) oferă o experiență colectivă impresionantă, ce cumulează peste 100 de ani. Această echipă experimentată este alcătuită din profesioniști care și-au perfecționat abilitățile în diverse sectoare, confruntându-se cu o serie de amenințări și incidente cibernetice. Aceștia oferă o înțelegere profundă și amplă, care le permite să identifice, să analizeze și să răspundă rapid incidentelor de securitate, păstrând în siguranță activele digitale ale clienților.

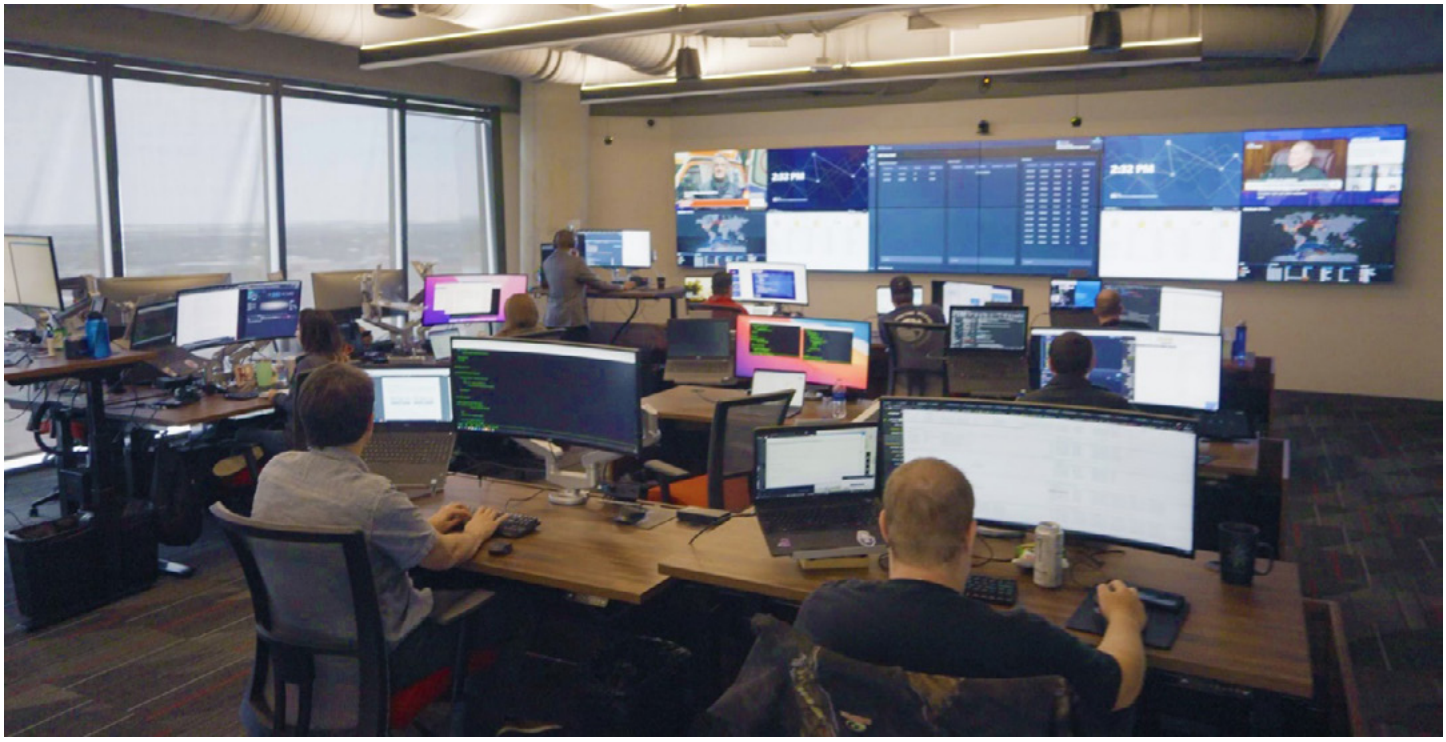


Figura 6: Cu sediul în San Antonio, Texas, Bitdefender NA SOC se mândrește cu un personal cu o bogată experiență în domeniul securității cibernetice.

Echipa de operațiuni Bitdefender MDR

Folosind vasta lor experiență, echipa noastră de operațiuni MDR navighează continuu în peisajul amenințărilor care continuă să evolueze, oferind soluții eficiente și practice pentru consolidarea posturii de securitate cibernetică a clienților noștri.

Analiști în securitate

Echipa Bitdefender Managed Detection & Response (MDR) este un grup de analiști de securitate cu o experiență bogată atât în domeniul securității cibernetice, cât și în aspecte mai largi ale tehnologiei informației. Fiecare membru al echipei deține o serie de certificări care atestă abilitățile și cunoștințele sale. Acestea includ o gamă diversă de acreditări SANS, cum ar fi GCFA, GFIH, GCDA, GDAT și GISP, printre altele. În plus, posedă certificări recunoscute internațional, cum ar fi CISSP, CEH, CCNA, OCSP, precum și suita CompTIA, inclusiv A+, Net+, Security+ și Pentest+.

Analiștii noștri contribuie nu doar cu priceperea lor tehnologică, ci și cu o experiență în diferite domenii. Acestea includ perioade de activitate în serviciile de informații militare, sisteme și administrare cloud și chiar în sferele de securitate națională. Acest fundal cu mai multe fațete le oferă o viziune unică, permițându-le să aducă perspective și soluții de securitate cibernetică de neegalat.

Echipă dedicată de cyber-intelligence

Avem o echipă dedicată de threat intelligence pe care o numim Cyber Intelligence Fusion Cell (CIFC). Experiența analiștilor de threat intelligence nu se limitează la amenințările cibernetice, deoarece mulți dintre angajați au ani de experiență în informațiile militare sau știința datelor. Echipa CIFC evaluează informațiile colectate dintr-o mare varietate de surse, inclusiv din diverse instrumente de colectare a informațiilor cibernetice, analiza Dark și Deep Web, colectarea de date din diverse surse de informații din comunitatea de securitate, cum ar fi forțele de ordine, alți cercetători de securitate și furnizorii de informații din întreaga lume, combinând informațiile despre amenințări de la echipa Bitdefender Labs și revizuind informații de la diferite agenții de știri de încredere.

Echipa de threat intelligence verifică un volum mare de date și le analizează pentru a extrage informații relevante și care pot genera acțiuni. Aceste informații ajută echipa de securitate să abordeze și să se pregătească pentru varietatea de amenințări care vizează în mod activ sau ar putea viza clienții Bitdefender. Echipa identifică tendințele care îi ajută să facă deducții informate și să fie cu un pas înaintea atacatorilor cibernetici. Însă analiza lor nu se limitează doar la securitatea cibernetică, aceștia examinând și știrile din domeniul business și geopolitic care pot avea un impact asupra securității cibernetice.

Pentru a organiza datele, echipa folosește instrumente de management al evenimentelor de securitate și informații (SIEM), o platformă de orchestrare, automatizare și răspuns de securitate (SOAR) și platforma GravityZone pentru a identifica datele semnificative. Analiștii din domeniul threat intelligence vor pune datele în context în beneficiul clienților MDR PLUS și vor ajuta la eliminarea rezultatelor fals pozitive, ambiguității și eforturilor dublate. Analiștii din domeniul threat intelligence dezvoltă acțiuni de intelligence hunting pentru clienții MDR PLUS, care sunt adaptate acestora în funcție de mediul, tendințele în materie de amenințări sau metodele potențiale de atac. Nu în ultimul rând, în timpul unui incident de securitate, echipa de threat intelligence le oferă sprijin analiștilor Bitdefender MDR SOC pentru a dezvolta acțiuni suplimentare de threat intelligence și pentru a investiga indicatorii de atac pentru ca mediul clienților să fie în siguranță.

Tehnologia noastră avansată

Serviciul Bitdefender Managed Detection & Response (MDR) valorifică avantajele platformei premiate GravityZone EDR și XDR.1Suita GravityZone, concepută meticulos pentru a răspunde mai multor tipuri de organizații, oferă un scut de securitate cibernetică ce include sisteme, rețele, e-mail, aplicații de productivitate, identități și sarcini de lucru în cloud.

Arhitectura suitei GravityZone se bazează pe o strategie de apărare în profunzime, îmbinând vizibilitatea și controlul într-o singură interfață de management holistică. De aici, profesioniștii noștri în securitate cibernetică pot monitoriza și gestiona eficient peisajul amenințărilor de securitate cibernetică specific unei organizații. Important este că această interfață de management oferă mijloacele pentru a investiga și a recupera în mod eficient datele în cazul unor incidente.

În centrul abordării multidimensionale a securității specifice GravityZone se află o combinație sofisticată de tehnologii de inteligență artificială și de machine learning, menite să protejeze organizațiile împotriva amenințările cibernetice cunoscute și emergente. Pentru a asigura un echilibru între detecția precisă a amenințărilor și reducerea la minimum a rezultatelor fals pozitive, perfecționăm constant algoritmii noștri inovatori. Astfel reducem resursele necesare pentru a securiza sistemele clientului. Optimizată special pentru medii cloud și virtuale, GravityZone asigură un impact minim asupra resurselor dvs. de cloud computing și asupra activelor virtualizate. Aceasta integrează senzori suplimentari în mediile dvs. hibride și multi-cloud pentru a eficientiza administrarea securității, prevenind în mod eficient breșele de securitate.

Funcționalitatea noastră nativă XDR oferă o acuratețe superioară a datelor și permite răspunsuri mai rapide la

1 Afirmație bazată pe date obținute din evaluări independente precum https://www.av-comparatives.org/, https://av-test.org, https://www.mrg-effitas.com/, https: //attackevals.mitre-engenuity.org/.

potențialele amenințări. Cu ajutorul senzorilor GravityZone XDR, echipa MDR poate înțelege rapid elementele cine, ce, când și cum ale unui atac și poate executa acțiuni de remediere fără întârzieri inutile cauzate de descifrarea surselor de date dezorganizate.

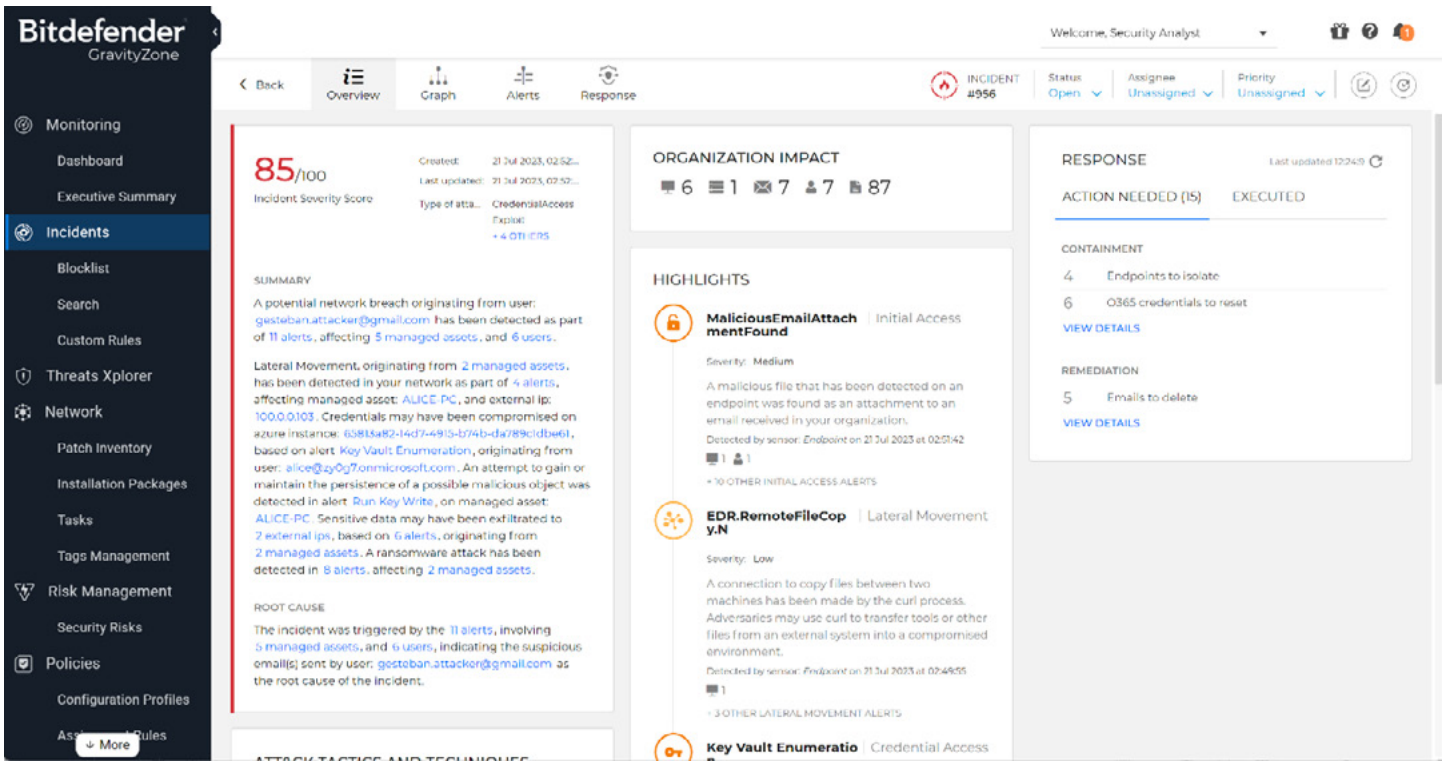


Figura 7: Cu ajutorul GravityZone XDR Incident Advisor, echipele de securitate pot evalua rapid detaliile importante ale unui incident, pentru a oferi un răspuns mai rapid.

Instrumente suplimentare

Echipa Bitdefender MDR folosește și alte instrumente pentru a efectua threat hunting în mediul clientului. În cadrul operațiunilor MDR, folosim platformele SIEM, SOAR și TIP pentru a interacționa cu mediul client. Toate datele care sunt create de alertele noastre EDR/XDR sunt păstrate în platforma noastră SIEM timp de 180 de zile în mod automat, ceea ce ne permite să desfășurăm activități foarte eficiente de threat hunting pe perioade de timp mai lungi. De asemenea, SIEM le permite analiștilor să cerceteze în profunzime evenimentele de securitate pentru a determina cauza principală a activității identificate.

De asemenea, în platformele Security Orchestration, Automation, & Response Platform (SOAR) și TIP se creează un model al amenințării. Modelul amenințării va conține toate informațiile cunoscute despre client și orice informații din surse deschise adunate de echipa de cyber intelligence. Aceste date ne permit, de asemenea, să creăm liste de monitorizare pe care echipa noastră de cyber intelligence le folosește pentru a tria alertele zilnic. Aceste alerte pot fi apoi convertite în solicitări de verificare a clienților sau acțiuni de threat hunting.

Sunt folosite instrumente brevetate personalizate, care ne permit să colectăm informații despre amenințări de la senzorii Bitdefender din întreaga lume. Alte instrumente externe sunt utilizate pentru a monitoriza Dark Web-ul, comunitățile Slack și Discord, blogurile de threat intelligence, GitHub, Pastebin, VirusTotal, Twitter și alte surse de informații privind securitatea cibernetică/criminalitatea cibernetică.

Portalul pentru clienți MDR

Portalul pentru clienți MDR oferă funcționalități care le permit clienților o modalitate mai bună de a urmări investigațiile MDR, acțiunile de threat hunting, rapoartele și cazurile, oferind în același timp un instrument de comunicare încrucișată

cu specialiștii GravityZone MDR SOC. Din portalul Bitdefender MDR, clienții pot consulta următoarele:

- **Tabloul de bord –** clienții pot revizui rapid grafice și statistici despre activități, progresul instalării, investigații, utilizatori și sistemele cele mai afectate, licențierea activă, datele colectate prin threat hunting și multe altele.
- **Secțiunea de activitate –** unde clienții pot urmări investigațiile și activitatea de threat hunting, inclusiv rezultatele analizei și recomandările.
- **Recomandări –** clienții pot examina recomandările privind activitățile de threat hunting și investigațiile furnizate de SOC Bitdefender MDR.
- **Tichete –** clienții pot folosi secțiunea de tichete pentru a deschide și monitoriza cazurile transmise analiștilor MDR Security.
- **Rapoarte –** această secțiune le permite clienților să acceseze diferitele rapoarte furnizate de echipa Bitdefender MDR.
- **Documente –** clientul și echipa MDR pot face aici schimb de informații valoroase, cum ar fi capturi de ecran, jurnale și multe altele.
- **Managementul serviciilor –** clienții pot configura cu ușurință informațiile de contact în caz de urgență și acțiunile preaprobate, precum și să completeze sau să actualizeze Chestionarul pentru clienți.
- **Utilizatori –** aici pot fi create și gestionate conturi suplimentare pentru utilizatorii cărora li se oferă acces la Portalul MDR. Trei roluri diferite pot fi atribuite utilizatorilor:
  - **Administrator –** acces complet la Portalul MDR.
  - **Utilizator –** poate încărca documente, poate trimite tichete și poate confirma investigațiile.
  - **Read-Only –** acces limitat numai pentru citirea datelor afișate în portal, fără posibilitatea de interacțiune ulterioară.
- **Companii –** le permite partenerilor, MSP și MSSP să își deservească clienții folosind serviciul MDR.

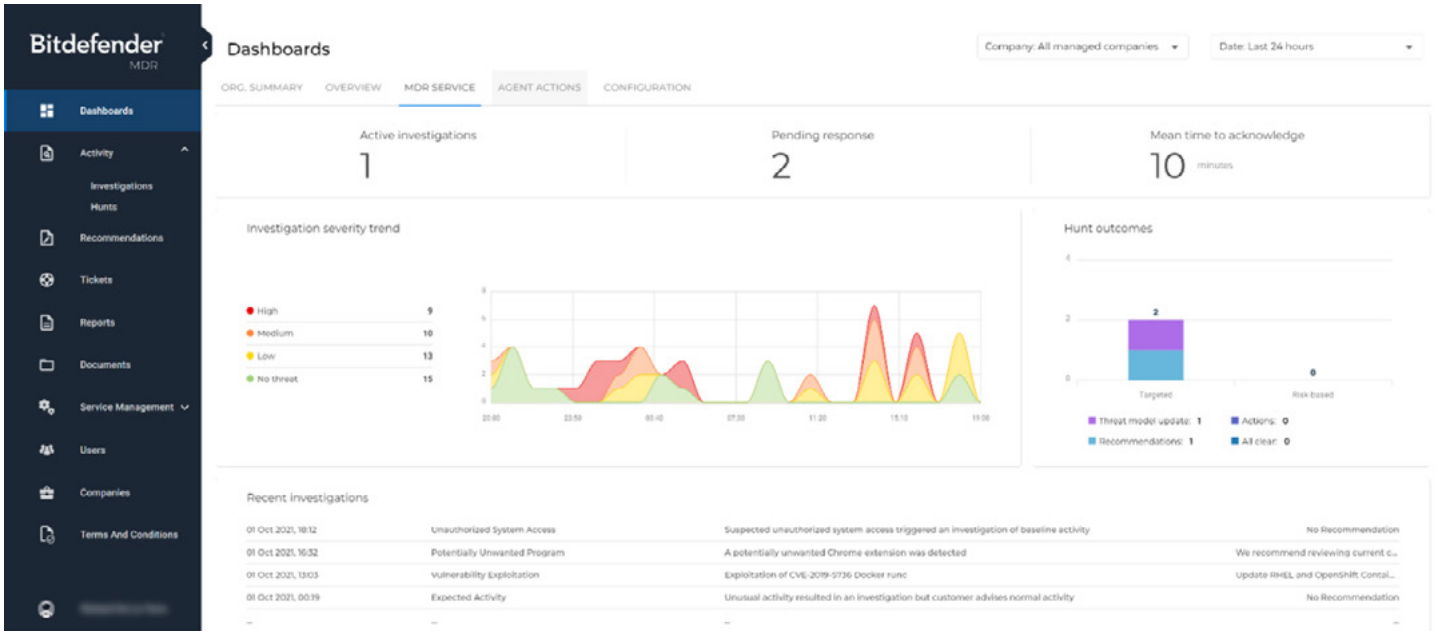


Figura 8: Folosind portalul Bitdefender MDR, clienții vor putea urmări activitatea de securitate cibernetică a echipei MDR, rapoartele de acces, rezultatele investigațiilor și multe altele.

Palmaresul nostru

Niciun alt furnizor de securitate cibernetică nu a fost cotat în mod constant pe prima poziție precum Bitdefender la testele independente2. Din 2018 până în 2023, Bitdefender a deținut prima poziție în proporție de 64% la testele privind prevenția atacurilor realizate de AV-Comparatives, ceea ce i-a determinat să ne catalogheze drept Strategic

2 Afirmație bazată pe date obținute din evaluări independente precum https://www.av-comparatives.org/, https://av-test.org, https://www.mrg-effitas.com/, https: //attackevals.mitre-engenuity.org/.

Leader în industrie.Rezultatele testului Business Security Test realizat de AV-Comparatives pentru perioada august – noiembrie 2023 arată că Bitdefender GravityZone oferă cea mai bună protecție dintre toți furnizorii evaluați, cu o rată de protecție de 100%. Excelăm la evaluările MITRE ATT&CK ®, având printre cele mai eficiente detecții analitice și continuăm să obținem premii de la alți evaluatori independenți, cum ar fi Forrester, MRG Effitas, AV-Test și nu numai.

Bitdefender MDR a fost desemnat „Representative Vendor" pentru a doua oară consecutiv în 2023 Gartner® Market Guide pentru servicii de detecție și răspuns administrate. Forrester a recunoscut, de asemenea, Bitdefender MDR drept „Notable Provider" în cadrul Managed Detection and Response Landscape, Q1 2023 și Managed Detection and Response Landscape în Europa, Q3 2023.

	Test scenarios														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Acronis	PRE	PRE	–	PRE	–	ON	–	ON	PRE	PRE	–	ON	–	–	–
Avast	POST	PRE	–	PRE	ON	ON	ON	ON	ON	ON	–	–	–	–	ON
Bitdefender	PRE	PRE	ON	PRE	ON	ON	ON	PRE	PRE	PRE	ON	PRE	PRE	–	POST
CrowdStrike	ON	ON	ON	ON	ON	ON	ON	ON	ON	POST	ON	–	–	–	–
ESET	POST	ON	PRE	PRE	ON	PRE	ON	POST	PRE	ON	PRE	–	ON	ON	ON
G Data	PRE	PRE	ON	PRE	POST	ON	–	PRE	PRE	ON	ON	PRE	ON	–	–
Kaspersky	PRE	ON	ON	ON	–	ON	–	POST	PRE	PRE	PRE	ON	–	ON	ON
Microsoft	PRE	PRE	PRE	PRE	ON	ON	PRE	–	ON	POST	PRE	–	PRE	–	–
VMware	PRE	ON	–	ON	–	ON	–	–	ON	PRE	–	ON	PRE	–	–

Figura 9: Testul detaliat de protecție avansată împotriva amenințărilor realizat de AV-Comparatives a arătat că Bitdefender a reușit să oprească mai multe atacuri în etapa de pre-execuție decât orice alt furnizor evaluat, iar rezultatele l-au determinat pe evaluator să comenteze: „O alarmă de efracție bună ar trebui să se declanșeze atunci când cineva intră în casa ta, nu atunci când începe să fure lucruri"

Bitdefender își dedică toate eforturile pentru a oferi cele mai bune tehnologii și servicii pentru combaterea criminalității cibernetice. Reputația noastră de a lideri în securitatea cibernetică ne-a permis să colaborăm cu agențiile de aplicare a legii din întreaga lume pentru a contracara organizațiile criminale responsabile pentru unele dintre cele mai dăunătoare atacuri ransomware, inclusiv Revil, Gandcrab și nu numai. Una dintre modalitățile prin care perturbăm activitatea acestor grupări Ransomware-as-a-Service este prin lansarea de instrumente de decriptare ransomware gratuite pe care oricine le poate descărca de pe labs.bitdefender.com. Aceste decriptoare le-au permis organizațiilor să-și recupereze datele criptate fără să plătească sume către aceste organizații criminale pentru cheile de decriptare și, făcând acest lucru, au deteriorat relațiile de încredere dintre furnizorii de ransomware și infractorii cibernetici care folosesc acest malware. Deși suntem dedicați să ajutăm publicul larg să lupte împotriva atacatorilor cibernetici, suntem cu mult mai dedicați să protejăm clienții care contează pe noi pentru a le proteja activele.

Asigurarea Bitdefender MDR în cazul producerii unei breșe de securitate cibernetică

În lupta fără sfârșit împotriva amenințărilor cibernetice, Bitdefender își propune să sprijine clienții în toate aspectele programului lor de securitate, diminuând orice preocupări ar avea aceștia în ceea ce privește impactul pe care îl creează incidentele cibernetice. De aceea, am colaborat cu Cysurance pentru a oferi o asigurare în cazul producerii unei breșe

de securitate cibernetică, fără costuri suplimentare, atât clienților MDR, cât și MDR PLUS. În cazul unui incident de securitate cibernetică, clienții MDR pot primi sprijin financiar pentru a-i ajuta la reducerea costurilor unei breșe de securitate.

În baza acestui acord, clienții Bitdefender MDR sunt eligibili pentru asistență financiară de până la 1.000.000 USD în cazul unui incident. Asigurarea Bitdefender MDR în cazul producerii unei breșe de securitate cibernetică este disponibilă la începutul unui nou abonament MDR sau pentru clienții MDR existenți până la sfârșitul contractului, după ce au examinat și acceptat termeni și condiții suplimentare. Pentru informații suplimentare,consultați Întrebările frecvente.

Acoperire	MDR	Acoperire	MDR PLUS sau MDR (peste 1000 de endpointuri)
Ransomware (inclusiv costurile/penalitățile asociate evenimentului)	$100,000	Total	$1,000,000
		Ransomware și eveniment BEC	$200,000
		Eveniment de conformitate	$200,000
		Eveniment de răspundere juridică cibernetică	$500,000
		Eveniment care afectează veniturile companiei*	$100,000*

**Acestui eveniment i se aplică o sumă deductibilă de 2.500 USD per solicitare*

Ce riscuri sunt acoperite?

Asigurarea Bitdefender MDR în cazul producerii unei breșe de securitate cibernetică, în parteneriat cu Cysurance, oferă asistență financiară pentru o gamă largă de costuri asociate incidentelor de securitate cibernetică, inclusiv:

- **Ransomware –** Ransomware, inclusiv remediere și solicitări de răscumpărare
- **Compromiterea adresei de e-mail de companie –** un eveniment BEC care are ca rezultat transferul de fonduri sau frauda cu facturi, inclusiv remedierea și pierderea de fonduri
- **Nerespectarea normelor de conformitate și a reglementărilor –** o breșă de securitate care declanșează încălcări ale HIPAA, PCI, OSHA și/sau ale prevederilor naționale și are ca rezultat o penalizare din partea autorităților de reglementare, o amendă sau cheltuieli aferente
- **Răspundere juridică cibernetică –** un proces care decurge dintr-un atac cibernetic, precum pierderea sau utilizarea abuzivă a datelor, sau un risc media legat de site-ul dvs. web în care apar costuri pentru apărarea juridică și pentru soluționare
- **Pierderea de venituri –** o breșă de securitate care are ca rezultat pierderea veniturilor din activități comerciale (profit net sau pierdere înainte de plata impozitelor pe profit) și/sau orice cheltuieli de exploatare ulterioare afectate de aceasta.

Servicii suplimentare

Pe lângă serviciile MDR, Bitdefender oferă și offensive services suplimentare, care vă ajută organizația să înțeleagă și să vizeze vulnerabilitățile asociate sistemelor, proceselor și angajaților. Bitdefender Offensive Services le oferă organizațiilor servicii de Penetration (Pen) Testing și Red Teaming pentru a se asigura că sunt identificate punctele slabe și vulnerabilități cheie de la nivelul securității pentru a îmbunătăți și a consolida securitatea mediilor dumneavoastră IT. Informații detaliate despre aceste servicii și nu numai sunt disponibile aici.

Offensive Security Services – Pen Testing

Bitdefender Pen Testing nu doar evaluează vulnerabilitățile, ci identifică și principalele puncte slabe ale securității astfel încât acestea să poată fi remediate, îmbunătățind astfel securitatea infrastructurii și, implicit, a organizației dvs.

Acest serviciu include operațiuni de tip penetration testing atât la nivel intern, cât și extern, identificând vulnerabilitățile din aplicațiile web și de mobil, rețele, aplicații de tip „thick client”, servicii web și API-uri și Wireless Access Points.

Fiecare mediu este unic, astfel încât specialiștii noștri în pen testing își adaptează metodele și vectorii de atac la fiecare situație.

Vă punem la dispoziție o gamă largă de operațiuni de tip pen testing, printre care:

- Aplicații web
- Aplicații de mobil
- Servicii web / API
- Rețele (interne sau externe)
- Aplicații de tip „thick client”
- Wireless Access Points

Offensive Security Services – Red Teaming

Bitdefender Red Teaming este o evaluare bazată pe informații detaliate, ce simulează amenințări din viața reală pentru a demonstra cum ar putea încerca hackerii să compromită funcționalitățile de importanță critică și sistemele de bază ale organizației dvs.Aceasta identifică vulnerabilitățile securității (fizice și digitale) din organizație pentru a vă ajuta echipa de securitate să îmbunătățească capabilitățile de detecție și răspuns.

Cu ajutorul exercițiilor noastre de Red Teaming, organizațiile pot:

- Identifica calea (căile) de atac ce afectează active de importanță critică, ce ar putea exista în rețeaua lor
- Ajuta Blue Team să înțeleagă mai bine vizibilitatea efectivă și gradul de acoperire din perspectiva detecției pentru a identifica lacunele și/sau acorda prioritate dezvoltării unor noi reguli de detecție
- Permite Blue Team să câștige experiență și să gestioneze incidentele pe baza unui playbook intern de răspuns la incidente
- Să organizeze dezbateri și discuții constructive în cadrul Blue Team
- Să contribuie la dezvoltarea rezilienței și adaptabilității la nivelul tuturor operațiunilor de securitate, prin expunerea la diferite puncte de vedere și scenarii diferite
- Să construiască un business case pentru dezvoltarea de noi soluții sau alte cheltuieli cu securitatea

Studii de caz

Furnizorul de servicii pentru locuințe ridică ștacheta în ceea ce privește securitatea cibernetică pentru toate companiile din lume

Compania, un furnizor global de servicii de reparații pentru locuințe cu sediul în Marea Britanie, cu 8,4 milioane de clienți rezidenți, căuta să standardizeze capacitățile de securitate cibernetică și să creeze o vizibilitate centralizată asupra infrastructurii operațiunilor sale federate din Europa, America de Nord și Asia.

Directorul responsabil cu securitatea informațiilor la nivelul grupului explică: „Am vrut să îmbunătățim controlul asupra riscului nostru de securitate cibernetică, având în vedere amenințările tot mai mari și să trecem la o forță de muncă cu un regim de lucru de la distanță. Modelul de business distribuit devenise un factor pe care trebuia să îl luăm în considerare în alegerea produsului potrivit. În plus, am vrut să îmbunătățim nivelurile diferite de expertiză și soluții în domeniul securității cibernetice din unitățile noastre de gestionate independent, indiferent de dimensiunea acestora.”

Pentru a îndeplini aceste obiective, compania și-a standardizat mediul de securitate cibernetică optând pentru Bitdefender Managed Detection & Response (MDR) PLUS.

„După evaluarea și testarea mai multor soluții de securitate cibernetică, am decis să consolidăm toate operațiunile noastre globale cu ajutorul Bitdefender MDR”, își amintește CISO la nivel de grup. „În timpul testării, am fost impresionați de capacitățile puternice de prevenție a atacurilor de tip exploit ale Bitdefender MDR în comparație cu

celelalte soluții. Calitatea expertizei echipei de securitate Bitdefender și natura colaborativă a relației pe care am stabilit-o cu Bitdefender au fost, de asemenea, factori în alegerea produsului.”

Faceți clic aici pentru a citi întregul studiu de caz.

Un furnizor de servicii de asistență medicală optează pentru un serviciu de monitorizare a securității și protecție 24x7 la un cost cu 40% mai mic decât costul aferent angajării de personal suplimentar

Pe măsură ce amenințările la adresa securității cibernetice continuă să se răspândească, departamentele de operațiuni de securitate internă ale organizațiilor din întreaga lume trebuie să aloce resurse semnificative pentru gestionarea și analizarea unui flux continuu de alerte și notificări. Pentru a face față acestei provocări, Magrabi Hospitals and Centers, un important furnizor de asistență medicală din Arabia Saudită, a luat în considerare angajarea mai multor persoane care să fie responsabile cu operațiunile de securitate pentru a asigura monitorizarea 24x7.

În schimb, Magrabi a stabilit că externalizarea către un serviciu de detecție și răspuns la nivelul endpointurilor administrate ar oferi o protecție mai completă și la un cost mai mic. Magrabi a evaluat ofertele de servicii administrate de detecție și răspuns de la Crowdstrike și Bitdefender și a selectat Bitdefender Managed Detection and Response (MDR).

Mostafa Mabrouk, Corporate Information Security Manager, Magrabi Hospitals and Centers, explică: „Am ales Bitdefender MDR pentru că ne oferea funcționalități complete de control, detecție, analiza informațiilor, raportare și protecție la nivelul endpointurilor. Pentru noi a fost foarte important să putem vizualiza toate componentele de securitate dintr-o singură consolă – de la eliminarea programelor malware la sandbox, carantină, jurnale și nu numai. De asemenea, am fost impresionați de expertiza și cunoștințele aprofundate ale analiștilor de securitate din cadrul echipei Bitdefender MDR.”

Faceți clic aici pentru a citi întregul studiu de caz.

Informații de contact

↳ Pentru a afla mai multe despre serviciile Bitdefender MDR, vă rugăm să ne contactați folosind Formularul de solicitare de informații despre MDR.

Asistență

↳ **Portalul de asistență tehnică pentru companii**

https://www.bitdefender.com/business/support/?lang=en

↳ **Date de contact ale echipei de asistență tehnică pentru companii**

https://www.bitdefender.com/business/support/en/71263-85158-contact.html

↳ **Politici Enterprise Support**

https://www.bitdefender.com/site/view/enterprise-support-policies.html

Bitdefender este un lider recunoscut în domeniul securității IT, care oferă soluții superioare de prevenție, detecție și răspuns la incidente de securitate cibernetică. Milioane de sisteme folosite de oameni, companii și instituții guvernamentale sunt protejate de soluțiile companiei, ceea ce face Bitdefender unul dintre cei mai de încredere experți în combaterea amenințărilor informatice, în protejarea intimității și datelor și în consolidarea rezilienței la atacuri. Ca urmare a investițiilor susținute în cercetare și dezvoltare, laboratoarele Bitdefender descoperă peste 400 de noi amenințări informatice în fiecare minut și validează zilnic in jur de 40 de miliarde de interogări privind amenințările. Compania a inovat constant în domenii precum antimalware, Internetul Lucrurilor, analiză comportamentală și inteligență artificială, iar tehnologiile Bitdefender sunt licențiate către peste 150 dintre cele mai cunoscute branduri de securitate din lume. Lansată în 2001, compania Bitdefender are clienți în peste 170 de țări și birouri pe toate continentele.

Sediul din România
Orhideea Towers
Șoseaua Orhideelor, nr. 15A,
sector 6,
București 060071
T: +40 21 4412452
F: +40 21 4412453

Sediul din SUA
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-BSG-MDR-SolutionGuide-creat8017-ro-RO
CD-09/17/24 • MD-September 17, 2024 8:04 pm