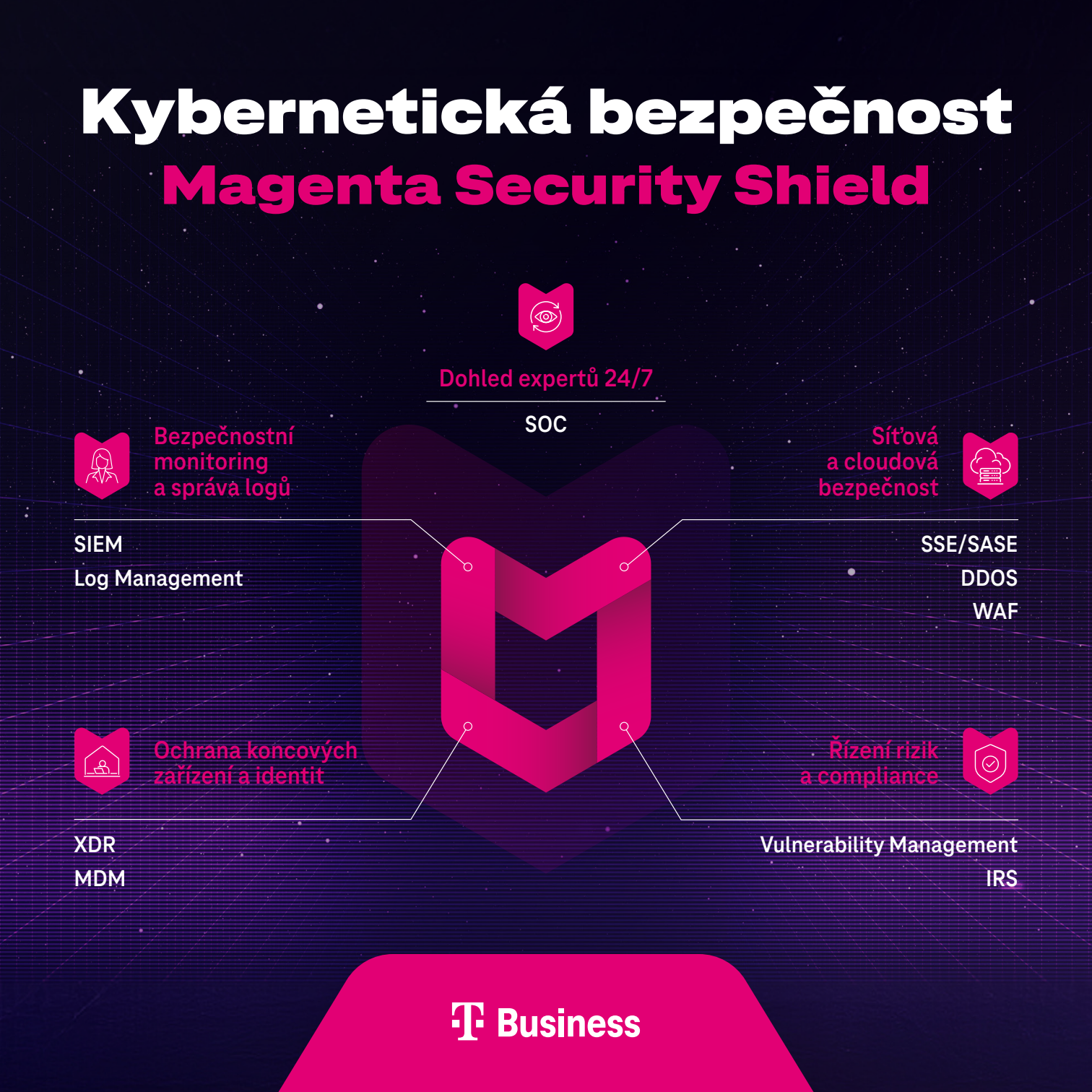
T Business

Magenta Security Shield

Komplexní kybernetická ochrana
na míru Vašim potřebám

Kybernetická bezpečnost

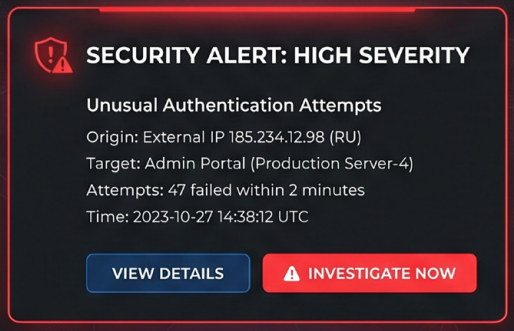
Magenta Security Shield



T Business

DOHLED EXPERTŮ 24/7

Firmy čelí stále složitějším kybernetickým hrozbám a bezpečnostní týmy jsou často přetížené, bez interních kapacit na nepřetržité sledování a rychlou reakci na incidenty. Zároveň se potýkají s velkým množstvím alertů, ve kterých je obtížné rozlišit kritické hrozby. Útoky přicházejí kdykoliv a i krátké zpoždění v reakci může vést k finančním ztrátám, výpadkům provozu nebo úniku dat.



Dokážete monitorovat a reagovat na kybernetické hrozby 24/7?

Firmy proto hledají způsob, jak tuto situaci efektivně zvládnout bez nutnosti budovat rozsáhlé interní kapacity. Využití Security Operations Center (SOC) jim umožňuje delegovat bezpečnostní dohled na specializovaný tým, který nepřetržitě vyhodnocuje události a pomáhá prioritizovat skutečně důležité hrozby. SOC zároveň poskytuje odbornou podporu při řešení incidentů a zajišťuje, že reakce na ně probíhá rychle a koordinovaně. Díky tomu organizace získává vyšší úroveň bezpečnosti, lepší přehled o rizicích a možnost soustředit se na své klíčové aktivity, aniž by musela investovat do vlastního 24/7 bezpečnostního týmu.

Naše řešení

24×7 dohled

Naše SOC služba zajišťuje kontinuální monitoring bezpečnostních událostí v reálném čase. Díky nepřetržitému dohledu dokážeme včas identifikovat potenciální hrozby a rychle na ně reagovat, ještě než způsobí škody — bez ohledu na denní dobu či vytížení vaší organizace. Služba zároveň pomáhá zajistit soulad s legislativními, regulatorními a bezpečnostními požadavky. V rámci ceny je zahrnut onboarding, pravidelné synchronizační schůzky či reporting.

Tým profesionálů

Získáte přístup k týmu zkušených bezpečnostních analytiků a pokročilým analytickým nástrojům bez potřeby budovat a udržovat vlastní SOC. Služba je ideální pro organizace, které chtějí zvýšit úroveň bezpečnosti nebo posílit stávající kapacity bez vysokých personálních a provozních nákladů.

Klíčové přínosy našich služeb

- Nepřetržitý dohled 24/7/365
- Rychlá detekce a reakce na hrozby
- Tým zkušených SOC analytiků se sídlem v ČR
- Podpora compliance a auditů
- Srozumitelný a pravidelný reporting
- Pokročilá analýza a korelace událost

MONITORING A SPRÁVA LOGŮ

Bez efektivního monitoringu a správy se logy z IT systémů rychle mění v nepřehlednou záplavu dat. Firmy bez centralizovaného log managementu postrádají přehled o dění v IT prostředí, odhalují incidenty pozdě a reagují až ve chvíli, kdy už vznikají škody. Roztříštěnost dat a složitá analýza zpomalují řešení problémů, komplikují audit a ztěžují plnění legislativních požadavků.



Máte přehled o svém IT prostředí a dokážete včas odhalit hrozby?

Pro získání přehledu v rostoucí komplexitě IT dat a minimalizaci zmíněných rizik je nezbytný efektivní Log Management. Ten centralizuje sběr logů a automatizuje jejich analýzu, čímž přeměňuje nepřehledná data v jasný obraz dění ve vašem IT prostředí. Díky tomu můžete aktivně chránit systémy, rychle odhalovat hrozby a efektivně optimalizovat provoz. Log Management tak tvoří základ, který lze elegantně rozšířit až na úroveň kompletního SIEM řešení pro proaktivní bezpečnostní operace a hlubokou analýzu incidentů.

Naše řešení

Log Management

Správa logů slouží ke sběru, centralizaci a správě systémových logů z celého IT prostředí. Umožňuje jejich přehlednou analýzu, rychlé vyhledávání a dlouhodobou archivaci, čímž podporuje včasnou detekci incidentů, zajištění souladu s předpisy a efektivní správu IT provozu. Naše služba Log Management zajišťuje kompletní péči – od dodávky a implementace infrastruktury přes pravidelný dohled a údržbu až po odborné konzultace.

Bezpečnostní monitoring

Monitoring staví na robustní SIEM platformě, která automaticky sbírá, koreluje a analyzuje bezpečnostní události z vašeho IT prostředí. Tyto informace jsou nepřetržitě sledovány našimi SOC (Security Operations Center) specialisty, což umožňuje včasnou detekci hrozeb, rychlou reakci na incidenty a efektivní ochranu organizace při zachování souladu s legislativními požadavky.

Klíčové přínosy našich služeb

- Centralizovaný přehled a kontrola IT dat na jednom místě
- Optimalizace IT provozu a výkonu
- Proaktivní detekce hrozeb a podezřelých aktivit
- Splnění compliance a usnadnění auditu
- Detailní podklady pro analýzu příčin a vyšetřování incidentů
- Podpora rozhodování s jasným pohledem na IT prostředí

SÍŤOVÁ A CLOUDOVÁ BEZPEČNOST

Útočníci dnes necílí pouze na data, ale i na samotnou dostupnost služeb. Využívají slabiny v síťové komunikaci a přístupu k aplikacím nebo cloudu, což vede k výpadkům, narušení provozu i únikům citlivých informací.



CLOUD SERVICE DISRUPTION
SECURITY ALERT

Jak ochránit síť, data i uživatele před rostoucími hrozbami?

Klíčem je posun od reaktivního řešení incidentů k proaktivní ochraně, která pokrývá celý životní cyklus síťové komunikace i přístupu k aplikacím a cloudu. To znamená nejen kontrolovat, kdo a odkud přistupuje, ale také průběžně vyhodnocovat provoz, odhalovat anomálie a v reálném čase reagovat na pokusy o zneužití či přetížení. Důležitá je i ochrana samotných aplikací před škodlivými požadavky a schopnost udržet jejich dostupnost i při zvýšené zátěži. Takový přístup umožňuje minimalizovat rizika, zajistit kontinuitu provozu a udržet důvěru zákazníků.

Naše řešení

Security Service Edge

Moderní ochrana síťové komunikace umožňuje bezpečný a řízený přístup uživatelů k aplikacím, datům a cloudu odkudkoliv. Řešení kombinuje řízení přístupů, průběžnou inspekci provozu a pokročilou ochranu před hrozbami. Zároveň umožňuje centralizovanou správu a jednotné bezpečnostní politiky. Ve službě je zahrnut návrh a implementace řešení, dodávka infrastruktury, podpora a pravidelnou optimalizaci.

DDoS ochrana

Udržení dostupnosti služeb i během cílených útoků je klíčové pro stabilní provoz a důvěru zákazníků. Naše řešení dokáže detekovat a mitigovat přetížení sítě a aplikací v reálném čase, minimalizuje dopad na provoz a zajišťuje, že kritické systémy zůstanou funkční. Služba zahrnuje návrh a implementaci ochranné infrastruktury, kontinuální monitoring, optimalizaci a odborné konzultace.

Webový aplikační firewall

Webové aplikace jsou častým cílem sofistikovaných útoků, proto je klíčové filtrovat škodlivý provoz a zajistit bezpečný přístup uživatelů. Naše řešení blokuje útoky na aplikační vrstvě, včetně nových hrozeb, bez dopadu na výkon či dostupnost. Součástí služby je návrh a implementace ochrany, kontinuální monitoring, aktualizace pravidel i odborné konzultace.

Klíčové přínosy našich služeb

- Proaktivní detekce hrozeb v reálném čase
- Minimalizace výpadků a zajištění kontinuity provozu
- Lokální podpora specialistů 24/7/365
- Centralizovaná správa a jednotné bezpečnostní politiky
- Špičková technologie ověřená v provozu
- Viditelnost a kontrola celého provozu sítě

OCHRANA KONCOVÝCH ZAŘÍZENÍ A IDENTIT

Většina bezpečnostních incidentů dnes začíná na koncových zařízeních, nad kterými firmy často nemají dostatečnou kontrolu. Tradiční antivirová ochrana dnes již nestačí a firmy tak čelí riziku nechráněného přístupu k firemním datům i aplikacím.



Jak ochránit koncová zařízení a identity před rostoucími hrozbami?

Řešením je získat viditelnost a kontrolu nad všemi endpointy, jako jsou servery, notebooky, počítače i telefony, a to bez ohledu na to, odkud zaměstnanci pracují. Jednoduchá správa, monitoring a ochrana zařízení i přístupových bodů k datům jsou nezbytné pro včasné odhalení podezřelého chování. Zároveň umožňují okamžitou reakci a zastavení útoku dříve, než se rozšíří napříč organizací. Naše XDR ochrana a správa mobilních zařízení pomocí MDM firmám poskytují potřebnou viditelnost, kontext, kontrolu i ochranu koncových bodů, a to i proti těm nejsofistikovanějším kybernetickým útokům.

Naše řešení

Ochrana stanic (XDR)

XDR technologie poskytuje ucelenou ochranu napříč koncovými zařízeními, uživatelskými identitami, sítí i cloudovým prostředím a přináší jednotný přehled o bezpečnosti celé organizace. Díky pokročilé korelaci dat z EDR, ochrany identit a dalších bezpečnostních vrstev dokáže řešení včas odhalit kompromitované účty, podezřelé chování i sofistikované cílené útoky a rychle na ně reagovat ještě předtím, než mohou negativně ovlivnit chod organizace nebo její business.

Správa zařízení (MDM)

Mobilní zařízení jsou častým cílem útoků. Proto je nezbytné mít plnou kontrolu nad jejich používáním, přístupem k firemním datům a dodržováním bezpečnostních politik. Řešení MDM umožňuje centrální správu a zabezpečení mobilních zařízení, ochranu firemních dat a bezpečný přístup uživatelů k aplikacím a systémům.

Klíčové přínosy našich služeb

- Proaktivní detekce a reakce na hrozby v reálném čase
- Ověřená řešení využívající AI a pokročilou analytiku
- Dohled zkušených specialistů 24/7
- Centralizovaná správa a jednotné bezpečnostní politiky
- Komplexní ochrana zařízení i uživatelů
- Snížení rizik a nákladů spojených s kybernetickými útoky

ŘÍZENÍ RIZIK A COMPLIANCE

V komplexním kybernetickém prostředí se řízení rizik a compliance bez jasné strategie mění v nepřehledný chaos. Absence celostního přístupu vystavuje organizaci hrozbám a zranitelnostem, narušuje provoz, přetěžuje interní týmy a zvyšuje riziko nesouladu s legislativou, vysokých sankcí i poškození reputace.



Získejte kontrolu nad riziky a buďte o krok napřed

Pro skutečnou kontrolu nad riziky a soulad s legislativou je nezbytná komplexní a proaktivní strategie. Ta vyžaduje důkladné porozumění aktuálnímu stavu vaší kybernetické bezpečnosti, systematickou identifikaci zranitelností, praviidelné testování připravenosti zaměstnanců na kybernetické hrozby a připravenost na rychlou a efektivní reakci na incidenty. Jen tak získáte jasný přehled o úrovni rizik, splníte legislativní požadavky, posílíte celkový bezpečnostní postoj organizace a proměníte rizika v dlouhodobou kybernetickou odolnost. Máme řešení, která vám s tímto procesem pomohou.

Naše řešení

Vulnerability Management

Komplexní řízení zranitelností proaktivně detekuje, analyzuje a eliminuje bezpečnostní slabiny napříč IT infrastrukturou, aplikacemi a systémy, pro zvýšení odolnosti vůči kybernetickým útokům a zajištění kontinuální bezpečnosti. Zahrnuje pravidelné skenování zranitelností pro identifikaci rizik, penetrační testy pro ověření jejich zneužitelnosti a analýzu rizík s prioritizací hrozeb. Tento přístup pomáhá s návrhem účinných protiopatření.

Incident Response Service

Kritické IT systémy a citlivá data jsou neustálým terčem sofistikovaných kybernetických útoků, proto je klíčové zajistit nejen preventivní ochrnau, ale i rychlou a kvalifikovanou reakci na vzniklé incidenty, minimalizujícií dopad na provoz. Naše služba Incident Response Service poskytuje proaktivní podporu při kybernetických incidentech. Zajišťuje efektivní zvládaní hrozeb a minimalizaci dopadů na provoz bez narušení výkonu a dostupnosti vašich systémů.

Klíčové přínosy našich služeb

- Jasný přehled o stavu kybernetické bezpečnosti a úrovni rizik
- Plnění legislativních požadavků (např. ZoKB)
- Vyšší připravenost na incidenty a rychlejší reakce
- Včasná identifikace a odstranění slabých míst
- Plynulejší a stabilnější provoz organizace
- Ochrana reputace a důvěryhodnosti organizace

T Business

