

BLACKCENSUS
POWERED BY CZECHAI

SECURITY INTELLIGENCE / BC-DEMO-001

BEZPEČNOSTNÍ AUDIT INFRASTRUKTURY

Ukázka technického reportu, plánu nápravy a manažerských výstupů pro zákazníky BLACKCENSUS.

DEMO	firma.example	v1.0
Modelový zákazník	Fiktivní doména	Vzor výstupu

OBSAH

01	Přehled	2	02	Rozsah	3
03	Metodika	4	04	Kontrolní matice	5–7
05	Registr nálezů	8	06	Detail nálezů	9–12
07	Plán nápravy	13	08	Návrh řešení a ceny	14
09	Manažerský výstup	15	10	Přehled dodávky	16

Provozovatel: A&L Prime s.r.o. (CzechAI), IČO 24009245, Zámostní 1155/27, 710 00 Ostrava, zapsaná u KS v Ostravě, sp. zn. C 101676 · ceo@czechai.io

UKÁZKOVÁ DATA • ŽÁDNÝ SKUTEČNÝ TEST • NEJDE O CERTIFIKACI

01 / PŘEHLED

STANDARD / 25 000 Kč

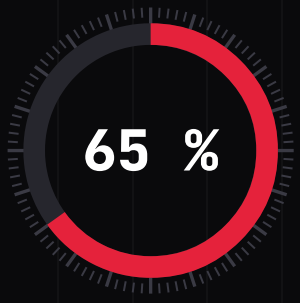
Bezpečnostní skóre

Ukázkový stav modelové firmy. Jedna číselná metrika, detailní pokrytí a jasné priority.

BLACKCENSUS SECURITY SCORE

65 / 100

PROSTOR PRO ZLEPŠENÍ



48	91 %	10
kontrol celkem	pokrytí relevantních kontrol	modelových nálezů

ROZLOŽENÍ NÁLEZŮ PODLE ZÁVAŽNOSTI

1	3	4	2
KRITICKÁ	VYSOKÁ	STŘEDNÍ	NÍZKÁ

Skóre podle oblastí

Webové stránky a aplikace	64	Doména, DNS a certifikáty	81
Síť a dostupné služby	58	Servery a provozní platformy	52
API a systémové integrace	62	Identity a přístupová oprávnění	49
Databáze a datová ochrana	70	Cloud a hosting	74
Monitoring a reakce na incidenty	62	Zálohy a obnova provozu	63
E-mail a komunikační bezpečnost	76	Řízení bezpečnosti a dokumentace	69

Vyhodnoceno 42 ze 48 kontrol, 4 neověřeny, 2 nerelevantní. Celkové skóre je průměr všech bodovaných kontrol, nikoli pravděpodobnost úspěšného útoku. Kritické nálezy se posuzují nezávisle na průměru.

02 / ROZSAH

STANDARD / 25 000 Kč

Co bylo zahrnuto do prověrky

Rozsah musí být před zahájením potvrzen elektronickou autorizací a ověřením oprávnění. Tento dokument používá výhradně fiktivní aktiva.

IDENTIFIKÁTOR	MODELOVÁ OBLAST	POKRYTÍ
A-01	Hlavní doména firma.example	Veřejné části webu
A-02	Dostupné podstránky a potvrzené subdomény	Autorizovaný rozsah
A-03	Související aplikační služby a integrace	Pouze potvrzená aktiva
A-04	Serverové a síťové prostředí	Veřejná expozice a doložené konfigurace
A-05	Databáze, cloud a identity	Rozsah dostupných důkazů
A-06	Provozní a bezpečnostní dokumentace	Modelově doložené podklady

Podmínky prověrky

AUTORIZACE

Objednatel elektronicky dokládá oprávnění k prověrce. Platba sama o sobě oprávnění nenahrazuje.

NEOHLÁŠENÝ TERMÍN

Přesný čas nemusí být znám běžnému IT týmu. Pověřený vlastník však prověrku schválil a existuje bezpečnostní kontakt.

OCHRANA PROVOZU

Bez neautorizovaných zásahů, destruktivních testů, narušování dostupnosti a kopírování dat nad nezbytný důkaz nálezu.

HRANICE A TŘETÍ STRANY

Cizí hosting, dodavatelé a další systémy se nezahrnují bez odpovídajícího oprávnění. Neveřejné části nelze plně ověřit bez podkladů.

Výstup zachycuje stav v okamžiku prověrky. Nejde o záruku, že systém neobsahuje další zranitelnosti, ani o prohlášení o souladu s konkrétním předpisem.

03 / METODIKA

STANDARD / 25 000 Kč

Jak číst hodnocení 0–100

Metodika BLACKCENSUS. V reálném reportu musí být každé hodnocení podloženo odpovídající evidencí.

SKÓRE	VÝZNAM	INTERPRETACE
90–100	**Silná ochrana**	Požadavek je převážně či plně doložen.
70–89	**Dobrá úroveň**	Ochrana funguje, existují dílčí nedostatky.
50–69	**Ke zlepšení**	Kontrola je splněna jen částečně.
25–49	**Slabá úroveň**	Významné nedostatky vyžadují nápravu.
0–24	**Závažná mezera**	Kontrola chybí nebo je zásadně nedostatečná.
NV	**Neověřeno**	Chybí přístup, podklady nebo důkaz; bez skóre.
NA	**Nerelevantní**	Kontrola se na rozsah nevztahuje; bez skóre.

Výpočet a pokrytí

CELKOVÉ SKÓRE

součet bodů 2737 / 42 bodovaných kontrol = 65.17 → 65/100
Oblast = průměr jejích bodovaných kontrol. Všechny kontroly mají v ukázce stejnou váhu.

POKRYTÍ

42 ověřených / 46 relevantních kontrol = 91 %
NV a NA se do skóre nezapočítávají; NV snižuje pokrytí.

Priorita nálezů (oddělená od skóre)

PRIORITA	ZÁVAŽNOST	DOPORUČENÁ REAKCE
P0	KRITICKÁ	Okamžitá triáž, bez zbytečného odkladu.
P1	VYSOKÁ	Přednostní řešení; orientačně do 7 dnů.
P2	STŘEDNÍ	Naplánovat nápravu; orientačně do 30 dnů.
P3	NÍZKÁ	Zařadit do běžného plánu; orientačně do 90 dnů.

Lhůty jsou modelové cíle nápravy, nikoli smluvní SLA. Závažnost se odvozuje z dopadu, pravděpodobnosti, dostupných důkazů a kontextu organizace.

BLACKCENSUS
POWERED BY CZECHAI

CZECHAI / SECURITY ASSURANCE
BC-DEMO-001

04 / KONTROLNÍ MATICE • 1/3

STANDARD / 25 000 Kč

Detailní výsledky kontrol

Každý řádek reprezentuje jednu modelovou kontrolu. Uvedené skóre není výsledkem skutečného testování.

WEB Webové stránky a aplikace

64 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
WEB-01	Bezpečnostní nastavení webu	65	Dílčí nedostatky v bezpečnostní konfiguraci. [F-05]
WEB-02	Ochrana uživatelských dat	78	Modelová dokumentace popisuje ochranné zásady.
WEB-03	Správa aplikačních změn	55	Neúplná evidence kontrol před nasazením. [F-06]
WEB-04	Ošetření chybových stavů	60	Nekonzistentní pravidla pro veřejné chybové výstupy. [F-09]

DNS Doména, DNS a certifikáty

81 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
DNS-01	Správa domén a subdomén	70	V evidenci je část položek bez potvrzeného vlastníka. [F-10]
DNS-02	Certifikáty a jejich životní cyklus	92	Modelová evidence expirací a obnovy je úplná.
DNS-03	Zabezpečení přenosu	85	Zásady šifrovaného přenosu jsou převážně splněny.
DNS-04	Ochrana doménových účtů	78	Odpovědnosti a revize přístupů jsou popsány.

NET Síť a dostupné služby

58 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
NET-01	Evidence dostupných služeb	45	Část služeb nemá doložené zdůvodnění a vlastníka. [F-04]
NET-02	Pravidla síťové ochrany	60	Doklady o pravidelném přezkumu nejsou úplné.
NET-03	Oddělení interních sítí	NV	Bez důkazů o interní konfiguraci.
NET-04	Správa změn síťových pravidel	70	Existuje postup, chybí část historie schválení.

SRV Servery a provozní platformy

52 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
SRV-01	Správa bezpečnostních aktualizací	30	Modelová evidence ukazuje opožděné nápravy. [F-03]
SRV-02	Bezpečnostní konfigurace	55	Chybí jednotný standard a potvrzení odchylek. [F-03]
SRV-03	Evidence zařízení a vlastníků	72	Inventář existuje, část údajů je neúplná.
SRV-04	Ochrana pracovních stanic	NA	V modelovém rozsahu nejsou koncové stanice.

04 / KONTROLNÍ MATICE • 2/3

STANDARD / 25 000 Kč

Detailní výsledky kontrol

Každý řádek reprezentuje jednu modelovou kontrolu. Uvedené skóre není výsledkem skutečného testování.

API API a systémové integrace

62 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
API-01	Pravidla přístupu k API	42	Dokumentace přístupových pravidel je neúplná. [F-05]
API-02	Životní cyklus integračních identit	65	Proces obnovy a rušení oprávnění je dílčí.
API-03	Monitoring integračních chyb	58	Neúplná evidence vyhodnocování událostí. [F-07]
API-04	Správa verzí rozhraní	85	Pravidla pro podporované verze jsou popsána.

IAM Identity a přístupová oprávnění

49 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
IAM-01	Vícefaktorová autentizace	15	V modelové evidenci není povinná pro všechny privilegované role. [F-01]
IAM-02	Revize privilegovaných oprávnění	35	Není doložena pravidelná revize vybraných rolí. [F-02]
IAM-03	Proces rušení účtů	70	Postup existuje, úplnost kontroly je dílčí.
IAM-04	Bezpečnost správy relací	75	Základní ochranné požadavky jsou popsány.

DB Databáze a datová ochrana

70 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
DB-01	Přehled datových úložišť	75	Evidence pokrývá modelové aplikační služby.
DB-02	Interní oprávnění k datům	NV	Nebyl poskytnut autorizovaný přístup ani důkazy.
DB-03	Pravidla klasifikace dat	55	Klasifikační pravidla nejsou doložena u všech systémů. [F-08]
DB-04	Zásady uchovávání dat	80	Modelová dokumentace pokrývá běžný životní cyklus.

CLD Cloud a hosting

74 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
CLD-01	Evidence cloudových prostředků	70	Seznam existuje, pravidelné revize jsou dílčí.
CLD-02	Přístupové zásady cloudu	NV	Interní nastavení poskytovatele není doloženo.
CLD-03	Odpovědnosti mezi dodavateli	85	Modelový přehled sdílené odpovědnosti je dostupný.
CLD-04	Evidence závislostí	68	Část závislostí nemá přiřazeného vlastníka. [F-10]

BLACKCENSUS
POWERED BY CZECHAI

CZECHAI / SECURITY ASSURANCE
BC-DEMO-001

04 / KONTROLNÍ MATICE • 3/3

STANDARD / 25 000 Kč

Detailní výsledky kontrol

Každý řádek reprezentuje jednu modelovou kontrolu. Uvedené skóre není výsledkem skutečného testování.

LOG Monitoring a reakce na incidenty

62 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
LOG-01	Pokrytí bezpečnostními logy	45	Není doloženo úplné pokrytí kritických služeb. [F-07]
LOG-02	Vyhodnocování upozornění	55	Evidence vyhodnocení není jednotná. [F-07]
LOG-03	Kontaktní role pro incidenty	80	Role a kontaktní kanály jsou určeny.
LOG-04	Pravidla ochrany auditních záznamů	70	Zásady existují, část potvrzení chybí.

BCP Zálohy a obnova provozu

63 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
BCP-01	Evidence zálohování	85	Modelový seznam zálohovaných služeb je k dispozici.
BCP-02	Ověření obnovitelnosti	35	Chybí aktuální doložený výsledek zkoušky obnovy. [F-06]
BCP-03	Odpovědnosti při výpadku	70	Odpovědnosti jsou popsány, revize je neúplná.
BCP-04	Interní ochrana kopií	NV	Bez ověřených podkladů o vnitřní konfiguraci.

MAIL E-mail a komunikační bezpečnost

76 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
MAIL-01	Zásady doménové e-mailové ochrany	82	Základní modelová ochrana je evidována.
MAIL-02	Ochrana firemních účtů	75	Zásady existují, jejich plošnost nebyla zcela doložena.
MAIL-03	Proces hlášení podezřelých zpráv	70	Proces je dostupný, pravidelná revize je dílčí.
MAIL-04	Testování zaměstnanců	NA	Sociální inženýrství není součástí tohoto produktu.

GOV Řízení bezpečnosti a dokumentace

69 /100

ID	KONTROLA	BODY	MODELOVÝ VÝSLEDEK
GOV-01	Evidence bezpečnostních rizik	60	Rizika nejsou sjednocena do jednoho registru. [F-08]
GOV-02	Přiřazení vlastníků systémů	65	Některé položky nemají potvrzeného vlastníka. [F-10]
GOV-03	Proces schvalování změn	80	Proces je popsán, dílčí doklady chybí.
GOV-04	Evidence uzavření nálezů	72	Historie náprav existuje, chybí jednotné potvrzení.

05 / REGISTR NÁLEZŮ

STANDARD / 25 000 Kč

Přehled identifikovaných rizik

Registr spojuje jednotlivé kontroly se zjištěními. Jeden nález může vysvětlovat více bodovaných kontrol.

ID	ZÁVAŽNOST	NÁLEZ	OBLAST	PRIORITA
F-01	KRITICKÁ	**Nedostatečná ochrana privilegovaných identit**	IAM	P0
F-02	VYSOKÁ	**Neúplná revize přístupových oprávnění**	IAM	P1
F-03	VYSOKÁ	**Zpožděná bezpečnostní údržba**	SRV	P1
F-04	VYSOKÁ	**Neúplné řízení dostupných služeb**	NET	P1
F-05	STŘEDNÍ	**Nekonzistentní aplikační zásady**	WEB / API	P2
F-06	STŘEDNÍ	**Nedoložené ověření obnovy a změn**	BCP / WEB	P2
F-07	STŘEDNÍ	**Neúplné pokrytí monitoringem**	LOG / API	P2
F-08	STŘEDNÍ	**Nesjednocená klasifikace a evidence rizik**	DB / GOV	P2
F-09	NÍZKÁ	**Nekonzistentní chybové výstupy**	WEB	P3
F-10	NÍZKÁ	**Neúplné přiřazení vlastníků aktiv**	DNS / CLD / GOV	P3

Stav evidence

Vzor obsahuje deset fiktivních nálezů. V ostrém auditu bude každý nález označen jako potvrzený, k ověření nebo vyvrácený; případně doplněn o omezení a datum kontroly.

Kritický nález F-01 vyžaduje prioritu P0 i při relativně příznivém celkovém skóre. Toto pravidlo zabraňuje tomu, aby průměr skryl závažné individuální riziko.

06 / DETAIL NÁLEZŮ • 1/4

STANDARD / 25 000 Kč

Karty bezpečnostních nálezů

Vzor struktury: popis, dopad, reference na důkaz, prioritizace a směr nápravy.

F-01

KRITICKÁ / P0

Nedostatečná ochrana privilegovaných identit

ZJIŠTĚNÍ	Z modelové matice účtů vyplývá, že povinné vícefaktorové ověření není doloženo pro všechny privilegované role.
MOŽNÝ DOPAD	Vyšší riziko neoprávněného přístupu a závažného zásahu do provozu.
DŮKAZ	Doklad E-01: anonymizovaná ukázka matice přístupových zásad.
SMĚR NÁPRAVY	Zavést a kontrolovat povinné vícefaktorové ověření privilegovaných účtů.

Oblast: **IAM** | Navržená odpovědnost: **Správa identit**

F-02

VYSOKÁ / P1

Neúplná revize přístupových oprávnění

ZJIŠTĚNÍ	Modelová evidence neobsahuje potvrzení poslední pravidelné revize vybraných privilegovaných rolí.
MOŽNÝ DOPAD	Nadměrná nebo neaktuální oprávnění mohou zvyšovat rozsah škod při incidentu.
DŮKAZ	Doklad E-02: ukázka záznamu o revizi rolí.
SMĚR NÁPRAVY	Zavést odpovědnosti, cyklus revizí a doložené schvalování přístupů.

Oblast: **IAM** | Navržená odpovědnost: **IT / IAM**

F-03

VYSOKÁ / P1

Zpožděná bezpečnostní údržba

ZJIŠTĚNÍ	V modelové evidenci údržby chybí potvrzení včasného uzavření několika bezpečnostních požadavků.
MOŽNÝ DOPAD	Zvýšené riziko narušení důvěrnosti, integrity nebo dostupnosti služeb.
DŮKAZ	Doklad E-03: anonymizovaný registr údržby bez konkrétních verzí.
SMĚR NÁPRAVY	Stanovit lhůty náprav podle rizika a ověřovat jejich splnění.

Oblast: **SRV** | Navržená odpovědnost: **IT provoz**

06 / DETAIL NÁLEZŮ • 2/4

STANDARD / 25 000 Kč

Karty bezpečnostních nálezů

Vzor struktury: popis, dopad, reference na důkaz, prioritizace a směr nápravy.

F-04

VYSOKÁ / P1

Neúplné řízení dostupných služeb

ZJIŠTĚNÍ	Některé modelové položky inventáře služeb nemají potvrzeného vlastníka nebo zdůvodnění.
MOŽNÝ DOPAD	Obtížná správa vystavených služeb a nejasná odpovědnost za rizika.
DŮKAZ	Doklad E-04: modelový inventář dostupných služeb.
SMĚR NÁPRAVY	Doplnit vlastníky, revize potřebnosti a schvalování změn.

Oblast: **NET** | Navržená odpovědnost: **Síťová správa**

F-05

STŘEDNÍ / P2

Nekonzistentní aplikační zásady

ZJIŠTĚNÍ	Modelové doklady ukazují rozdílnou úroveň potvrzení bezpečnostních požadavků mezi aplikacemi a integracemi.
MOŽNÝ DOPAD	Zvýšená pravděpodobnost chyb při změnách a odlišná úroveň ochrany uživatelských dat.
DŮKAZ	Doklad E-05: ukázka porovnání bezpečnostních požadavků.
SMĚR NÁPRAVY	Sjednotit zásady a kontrolu jejich dodržování před vydáním změny.

Oblast: **WEB / API** | Navržená odpovědnost: **Vývoj / AppSec**

F-06

STŘEDNÍ / P2

Nedoložené ověření obnovy a změn

ZJIŠTĚNÍ	Modelové podklady neobsahují aktuální záznam o úspěšné zkoušce obnovy a úplné kontrole změn.
MOŽNÝ DOPAD	Možné prodloužení výpadku a komplikace obnovy po incidentu.
DŮKAZ	Doklad E-06: modelový záznam provozní připravenosti.
SMĚR NÁPRAVY	Zavést pravidelné dokladované ověřování obnovy a změn.

Oblast: **BCP / WEB** | Navržená odpovědnost: **IT provoz**

06 / DETAIL NÁLEZŮ • 3/4

STANDARD / 25 000 Kč

Karty bezpečnostních nálezů

Vzor struktury: popis, dopad, reference na důkaz, prioritizace a směr nápravy.

F-07

STŘEDNÍ / P2

Neúplné pokrytí monitoringem

ZJIŠTĚNÍ	Modelový přehled monitoringu neprokazuje úplné pokrytí kritických systémů a pravidelné vyhodnocování upozornění.
MOŽNÝ DOPAD	Pozdější zjištění incidentu a neúplné podklady pro jeho vyšetření.
DŮKAZ	Doklad E-07: ukázka matice monitoringu.
SMĚR NÁPRAVY	Doplnit inventář monitorovaných systémů a pravidla reakce.

Oblast: **LOG / API** | Navržená odpovědnost: **Bezpečnostní tým**

F-08

STŘEDNÍ / P2

Nesjednocená klasifikace a evidence rizik

ZJIŠTĚNÍ	Modelové dokumenty neobsahují jednotnou klasifikaci dat a centrální evidenci bezpečnostních rizik.
MOŽNÝ DOPAD	Nekonzistentní rozhodování o ochraně dat a prioritách investic.
DŮKAZ	Doklad E-08: modelový registr klasifikace a rizik.
SMĚR NÁPRAVY	Zavést jednotnou klasifikaci dat a registr rizik s vlastníky.

Oblast: **DB / GOV** | Navržená odpovědnost: **Risk / compliance**

> V reálném reportu by byly připojeny nezbytné a přiměřeně anonymizované důkazy. Citlivé technické podklady se předávají pouze oprávněným osobám zabezpečeným způsobem.

06 / DETAIL NÁLEZŮ • 4/4

STANDARD / 25 000 Kč

Karty bezpečnostních nálezů

Vzor struktury: popis, dopad, reference na důkaz, prioritizace a směr nápravy.

F-09

NÍZKÁ / P3

Nekonzistentní chybové výstupy

ZJIŠTĚNÍ	Modelová evidence popisuje odlišná pravidla pro zobrazení a evidenci chyb.
MOŽNÝ DOPAD	Nepřehledné chování aplikací a zhoršená správa provozních chyb.
DŮKAZ	Doklad E-09: modelová kontrola zásad chybových výstupů.
SMĚR NÁPRAVY	Sjednotit a pravidelně kontrolovat pravidla pro chybové výstupy.

Oblast: **WEB** | Navržená odpovědnost: **Vývoj**

F-10

NÍZKÁ / P3

Neúplné přiřazení vlastníků aktiv

ZJIŠTĚNÍ	Část modelového inventáře nemá doloženého vlastníka nebo aktuální stav revize.
MOŽNÝ DOPAD	Prodloužení řešení provozních nebo bezpečnostních problémů.
DŮKAZ	Doklad E-10: modelový výpis inventáře aktiv.
SMĚR NÁPRAVY	Doplnit odpovědnosti a zavést periodický přezkum inventáře.

Oblast: **DNS / CLD / GOV** | Navržená odpovědnost: **IT / správa aktiv**

> V reálném reportu by byly připojeny nezbytné a přiměřeně anonymizované důkazy. Citlivé technické podklady se předávají pouze oprávněným osobám zabezpečeným způsobem.

07 / PLÁN NÁPRAVY

ADVANCED / 50 000 Kč

Od zjištění ke konkrétním opatřením

Rozšířený výstup ADVANCED obsahuje prioritizaci, odpovědnosti, akceptační kritéria a návaznosti.

PRIORITA / ID	NAVRŽENÉ OPATŘENÍ	ODPOVĚDNOST	KRITÉRIUM SPLNĚNÍ
P0 / F-01	**Posílit ochranu privilegovaných identit**	IAM	Doložené plošné vynucení politiky.
P1 / F-02	**Revize rolí a schválení přístupů**	IT / IAM	Schválený a evidovaný seznam rolí.
P1 / F-03	**Zavést režim bezpečnostní údržby**	IT provoz	Přehled termínů a uzavřených náprav.
P1 / F-04	**Zrevidovat dostupné služby a odpovědnosti**	Síťová správa	Inventář se schváleným vlastníkem.
P2 / F-05	**Sjednotit aplikační bezpečnostní zásady**	Vývoj	Ověřený proces kontroly změn.
P2 / F-06	**Doložit připravenost na obnovu**	IT provoz	Záznam o ověření obnovy.
P2 / F-07	**Rozšířit pokrytí bezpečnostními logy**	Security	Potvrzená matice pokrytí a reakce.
P2 / F-08	**Sjednotit klasifikaci a řízení rizik**	Risk	Schválená klasifikace a registr rizik.
P3 / F-09	**Sjednotit správu chybových stavů**	Vývoj	Schválená pravidla a kontrola.
P3 / F-10	**Doplnit vlastníky aktiv**	IT	Úplná a aktualizovaná evidence.

Modelový harmonogram

0–7 dní

P0: bezodkladně; P1: přednostní stabilizace

8–30 dní

P2: systémová náprava a dokumentace

31–90 dní

P3: sjednocení procesů a průběžná kontrola

Harmonogram je ilustrativní. Cena balíčku zahrnuje zpracování návrhu a cenové nabídky, nikoli automaticky samotnou implementaci.

08 / NÁVRH ŘEŠENÍ A CENY

ADVANCED / 50 000 Kč

Bezpečnostní architektura na míru

Zákazník získá doporučené vrstvy ochrany, výběrová kritéria a ocenění případné implementace.

01	IDENTITA	Silné ověřování a řízení oprávnění
02	APLIKACE	Bezpečný životní cyklus webu a API
03	INFRASTRUKTURA	Správa aktiv, konfigurací a aktualizací
04	DETEKCE	Centralizace událostí a reakce na incidenty
05	ODOLNOST	Obnovitelnost a kontinuita provozu

Ukázková cenová nabídka implementace

ID	POLOŽKA	CENA (MODEL)
Q-01	Ochrana identit a přístupů	24 000 Kč
Q-02	Náprava konfigurací a evidence služeb	28 000 Kč
Q-03	Rozšíření monitoringu a procesů reakce	35 000 Kč
Q-04	Zavedení kontrol obnovy a změn	18 000 Kč
Q-05	Předání dokumentace a ověření opatření	15 000 Kč
CELKEM	**Jednorázová implementace**	120 000 Kč

Částky jsou výhradně ilustrativní, nejsou nabídkou ani tržním odhadem. Skutečná nabídka musí vycházet z ověřeného rozsahu nápravy, licencí, kapacity a režimu DPH. Průběžné služby a licence se oceňují zvlášť.

09 / MANAŽERSKÝ VÝSTUP

DEEP RED TEAM / 100 000 Kč

Rozhodovací podklady pro vedení

Pět prémiových rozšíření nad rámec kompletního STANDARD a ADVANCED.

HLAVNÍ MANAŽERSKÉ SDĚLENÍ

Prioritou je ochrana privilegovaných identit, řízení dostupných služeb a bezpečnostní údržba. Celkové skóre samo o sobě není důvodem k odložení kritické nápravy.



Pět výstupů navíc

1.	**Hloubková prověrka**	Rozšířené pokrytí a podrobnější posouzení autorizovaných částí infrastruktury; rozsah závisí na ověřitelných přístupech.
2.	**Expertní validace**	Odborné přezkoumání kritických a vysokých nálezů, kvality důkazů a rizik chybných závěrů.
3.	**Manažerský report**	Rozhodovací shrnutí pro vedení, priority, odpovědnosti, investice a akceptace zbývajících rizik.
4.	**Obchodní a finanční dopady**	Posouzení dopadů na kontinuitu, náklady obnovy, důvěrnost dat a reputaci; vyčíslení jen s doloženými vstupy.
5.	**Kontrolní prověrka**	Samostatné porovnání původních a nových zjištění po provedení nápravy. Stav otevřeno / částečně / uzavřeno / neověřeno.

Vzor kontrolního ověření

NÁLEZ	VÝCHOZÍ STAV	NOVÝ STAV	ROZHODNUTÍ
F-01	KRITICKÁ	Neověřeno	Otevřený do doložení nápravy
F-03	VYSOKÁ	Neověřeno	Čeká na kontrolu opatření
F-07	STŘEDNÍ	Neověřeno	Čeká na kontrolu opatření

Žádné výsledky opakované prověrky nejsou v tomto vzoru simulovány jako skutečně provedené. Termín opakované kontroly navazuje na dokončení nápravy a je oddělený od prvního auditu.

10 / PŘEHLED DODÁVKY

VŠECHNY TARIFY

Co přesně zákazník obdrží

Ukázkový report zahrnuje všechny tři úrovně. Níže je přehled obsahu podle zakoupeného balíčku.

VÝSTUP	25 000 KČ	50 000 KČ	100 000 KČ
Technický audit a rozsah	ANO	ANO	ANO
Security Score 0–100	ANO	ANO	ANO
Detailní matice všech relevantních kontrol	ANO	ANO	ANO
Registr nálezů a detailní karty	ANO	ANO	ANO
Důkazy a omezení prověrky	ANO	ANO	ANO
Priorita a základní směr nápravy	ANO	ANO	ANO
Komplexní plán a akceptační kritéria	–	ANO	ANO
Návrh moderní ochrany	–	ANO	ANO
Cenová nabídka implementace	–	ANO	ANO
Hloubková prověrka	–	–	ANO
Expertní validace	–	–	ANO
Manažerský report	–	–	ANO
Obchodní a finanční dopady	–	–	ANO
Kontrolní prověrka po nápravě	–	–	ANO

Předání a důvěrnost

Standard předání: PDF report, strojově čitelný registr kontrol a nálezů (CSV/XLSX) a přiměřené důkazní přílohy, dostupné pouze autorizovanému zákazníkovi. První audit do 10 dnů od ověření objednávky a oprávnění; opakovaná prověrka až po nápravě.

Provozovatel: A&L Prime s.r.o. (CzechAI), IČO 24009245, Zámostní 1155/27, 710 00 Ostrava, zapsaná u KS v Ostravě, sp. zn. C 101676 · ceo@czechai.io



Tento dokument je ukázka výstupu, nikoli audit, skutečný scan, certifikace ani závazná nabídka. Doména firma.example je fiktivní; výsledky, nálezy, důkazy a ceny nápravy jsou modelové.