GDPR ve Vaší organizaci.

Nestrašíme, pomáháme

Jiří Stich
Člen výkonného výboru CSCC

czech smart city cluster

Atos

Stávající členové CSCC



Vznik a poslání klastru

- CSCC byl založen 15.12.2015
- Zakládající členové
  - Atos IT Solutions and Services, Česká Spořitelna, ČVUT, E.ON, Schneider Electric a Technologické centrum Písek
- Poslání
  - Rozvoj jedinečného partnerství mezi firmami, státní správou, samosprávou, znalostními institucemi a obyvateli měst
  - Pomoc vedení měst a krajů s přípravou inovativních konceptů
  - Dohled nad realizovanými projekty
  - Vytvoření srozumitelné metodiky

GDPR - strašák nebo příležitost?

1. Plníte (snažíte se)122/2013 Z.z. a 164/2013 Z.z. ?
   Pak je GDPR jen trocha práce navíc (nové instituty)

2. Je pro Vás ochrana OÚ a ISO 27001 pouhé intelektuální cvičení?
   Pak Vás čeká dost práce

3. Je motivací stran GDPR tlak „zeshora“, nebo se obáváte svých zákazníků / dodavatelů / partnerů?

4. Zkusíte to sami, nebo s podporou Atosu? ☺

1 Právní analýza

2 Revize procesů

3 Datový audit

4 Report a návrh nápravných opatření

5 Zavádění opatření

1 Právní analýza

Tipy a Triky, na co si dát pozor

Právní (prvotní, dopadová) analýza by ruku v ruce měla jít s analýzou rizik.

A to jako proč?

Deklarovaný soulad s legislativou prostřednictvím skvěle zpracované, ale v prostředí nezavedené bezpečnostní politiky v organizaci se organizaci vymstí v podobě neschopnosti procesovat požadavky subjektů OÚ.

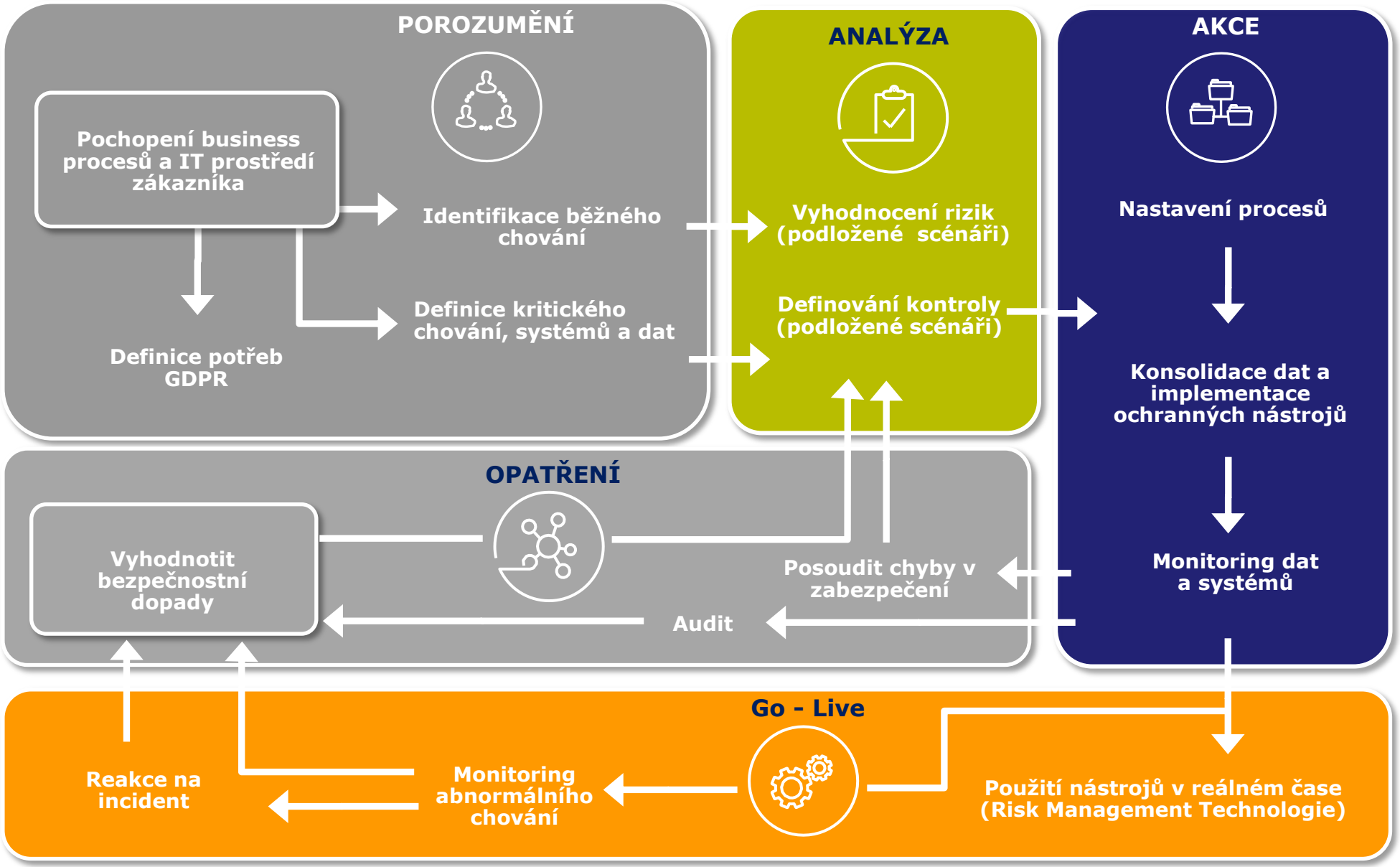
#	Požadavek	Ano	Ne	Částečně
1	Je zabezpečena ochrana perimetru Firewallem?	X		
2	Je zpracovaný akt formou směrnice stran řízení přístupu k informačním systémům?	X		
3	Máte vytvořenu politiku klasifikace dokumentů?	X		

A v reálném prostředí to vypadá jak?

Atos

2 Revize procesů

Máte popsány, nebo alespoň zmapovány Vaše procesy?



3 Datový audit

Hodnocení rizik GDPR dat

5 jednoduchých otázek

1. Jaká osobní data občanů EU máte v držení?
2. Jak citlivá data to jsou?
3. Kde se v rámci organizace tato nacházejí a kdo k nim přistupuje?
4. Jak se v organizaci pohybují, kam a kudy z organizace odcházejí?
5. Jak se s nimi pracuje a komu jsou poskytována?

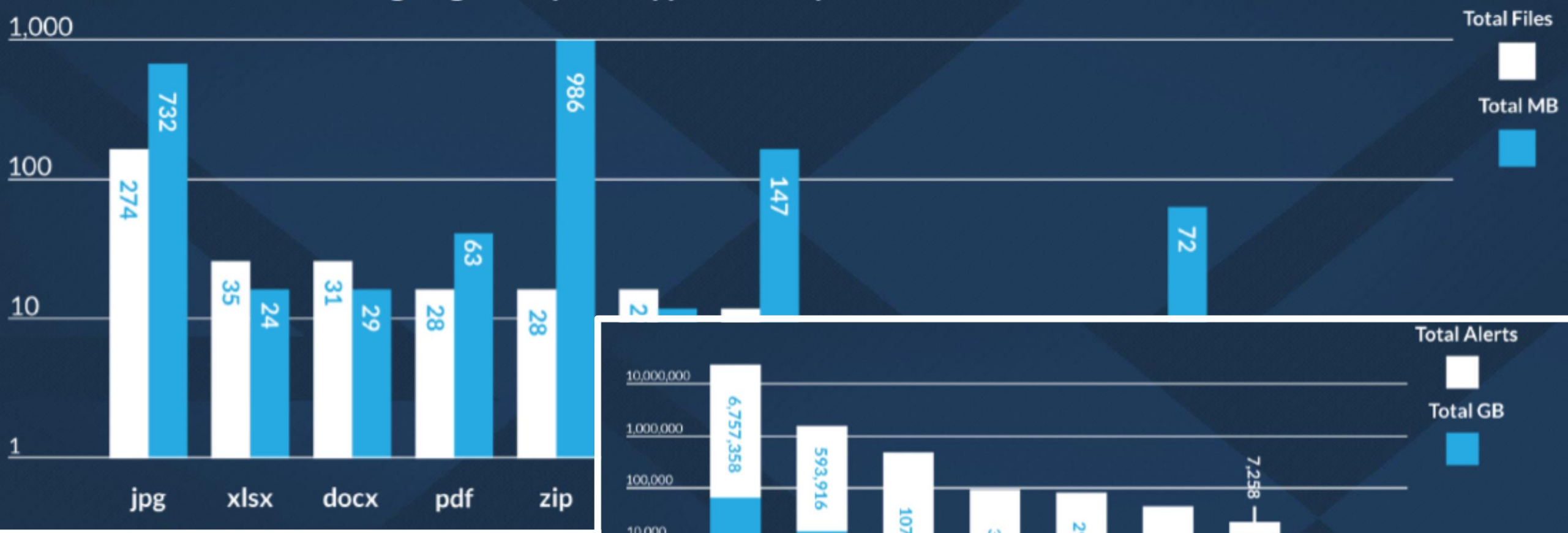
Fáze 1 - Analýza statických dat

Poznejte, kde jsou uložena Vaše osobní data

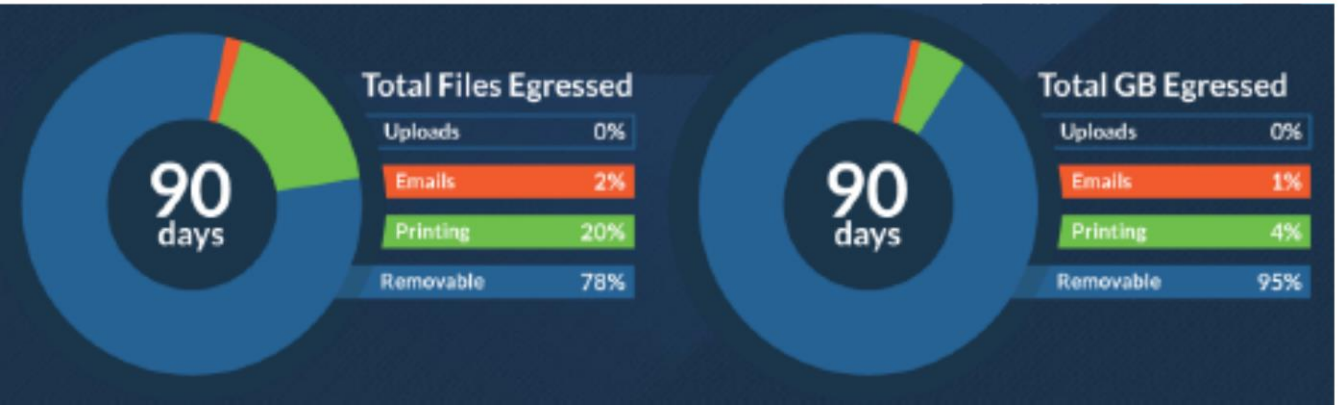
Tato analýza zahrnuje zjištění, detekování osobních dat občanů EU napříč Vaší datovou infrastrukturou, tedy síťovými úložišti, databázemi a cloudovými úložišti. Naše platforma má vestavěné politiky detekující datové vzory GDPR, nemusíte je tedy složitě definovat. Vlastní vzory GDPR dat typické pro Vaši organizaci Vám rádi nastavíme a budeme schopni detekovat jejich přítomnost jak na lokálních, síťových i cloudových úložištích.

Naše platforma „ATOS threat aware data protection" skenuje úložiště, která určíte za účelem identifikace:

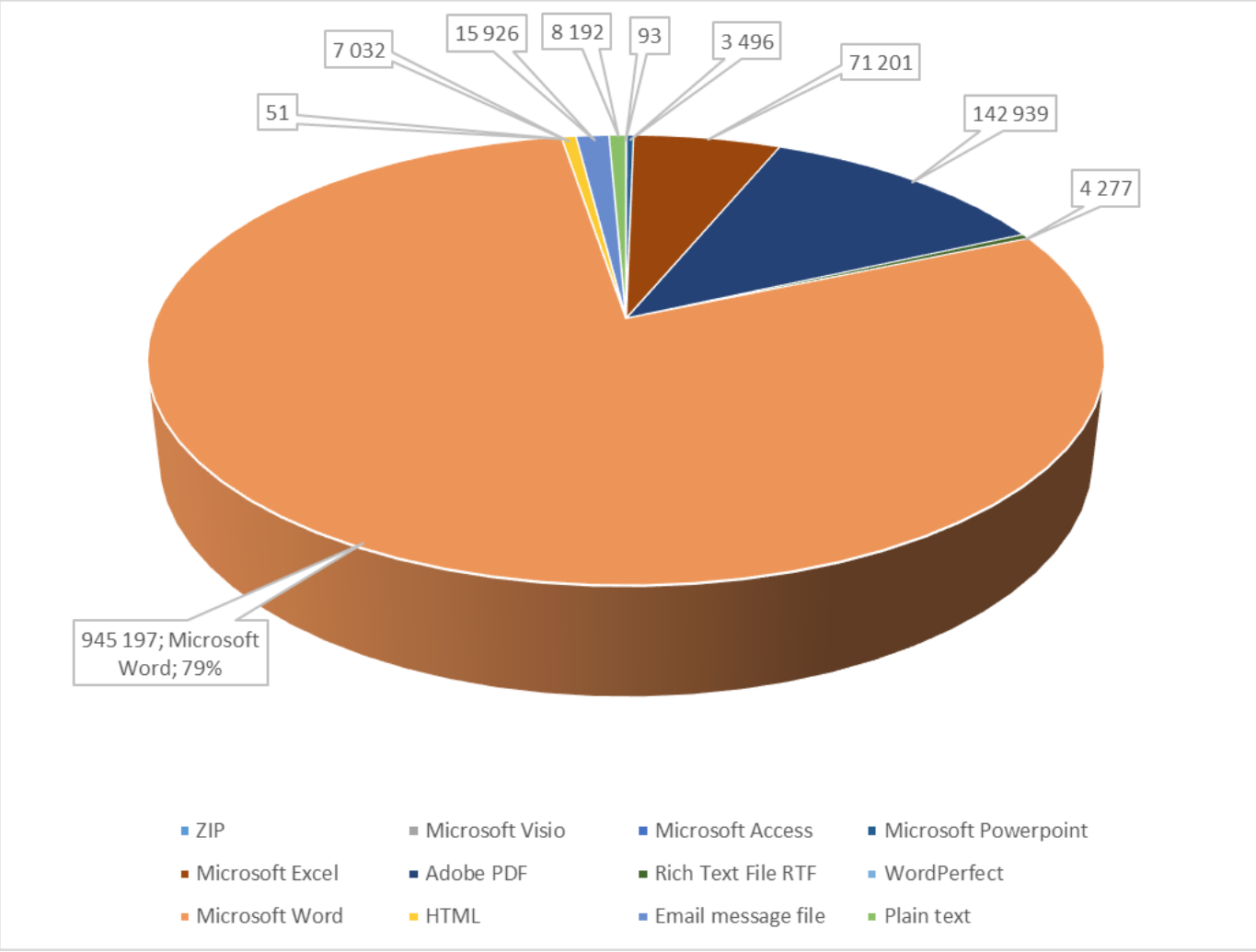
- Všech typů osobních dat
- Úrovní citlivosti těchto dat
- Která úložiště obsahují osobní data


1,000
100
10
1
Total Files
Total MB
274
732
35
24
31
29
28
63
28
986
2
147
72
jpg
xlsx
docx
pdf
zip

Total Alerts
Total GB
10,000,000
1,000,000
100,000
10,000
1000
6,757,358
12,072
593,916
5,918
107,408
73
30,505
108
29,058
123
18,793
63
7,258
6,126
5,293
21
Outlook Email
CD/ DVD
Home network
Uploads & Webmail
Outlook data file
Cloud uploads
Monitor
Monitor
Monitor
Prompt
Prompt
Block
Current State
Prompt
Prompt
Prompt
Block
Block
Block
Recommended State


90
days
Total Files Egressed
Uploads 0%
Emails 2%
Printing 20%
Removable 78%
90
days
Total GB Egressed
Uploads 0%
Emails 1%
Printing 4%
Removable 95%

Čísla z praxe – v jakých datech nacházíme osobní údaje



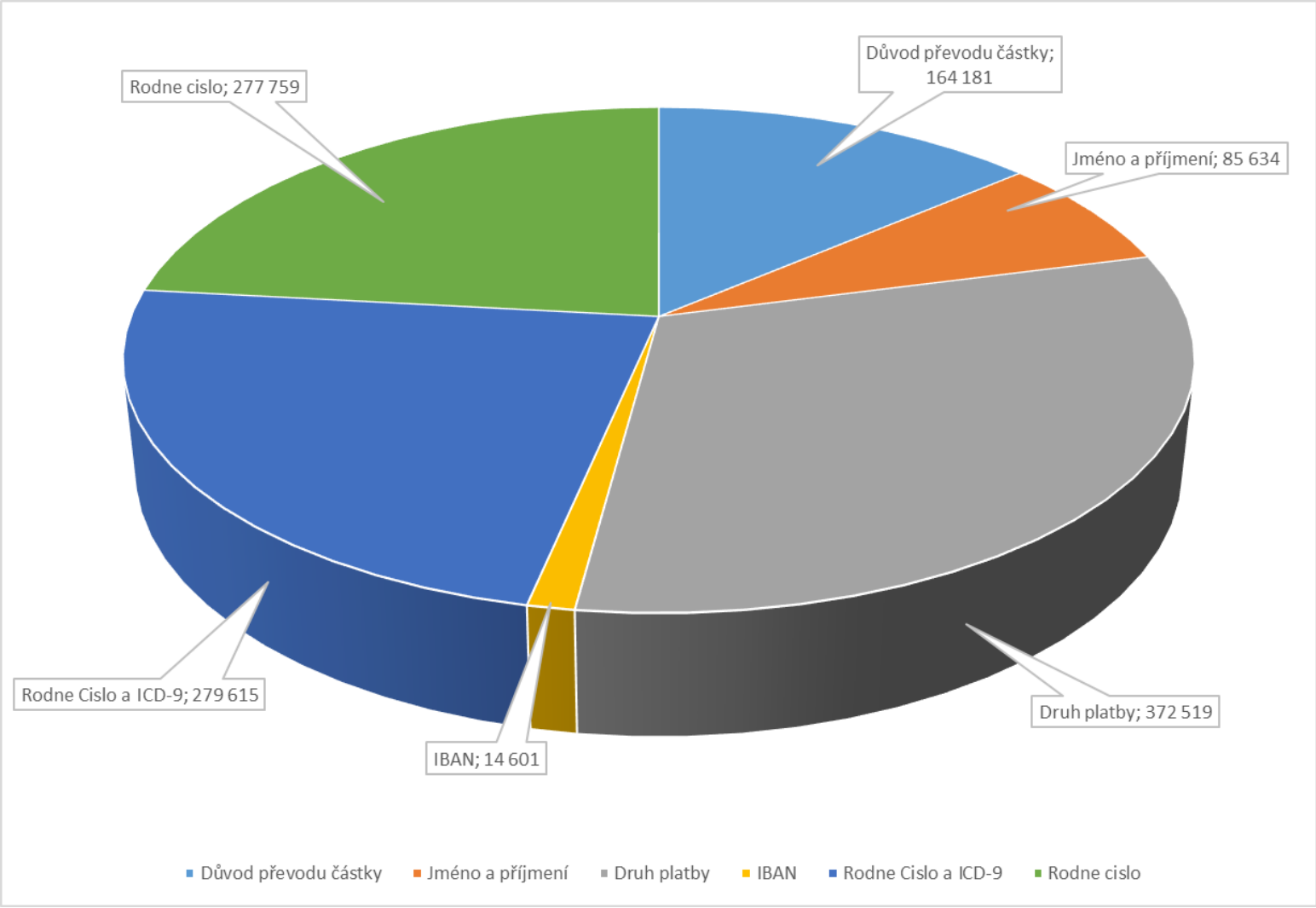
Zákazník z veřejné správy

Souborové úložiště

Celkem: 2 826 740 dokumentů

V 1 198 456 dokumentech byly detekovány 1 a více osobních údajů vč. citlivých osobních údajů

Čísla z praxe – jaké osobní údaje nacházíme



Zákazník z veřejné správy

Souborové úložiště

Celkem 18 550 425 dokumentů

V nich nalezeno celkem v různých kombinacích 59 556 747 osobních a citlivých osobních údajů

Fáze 2 - Analýza dat v pohybu

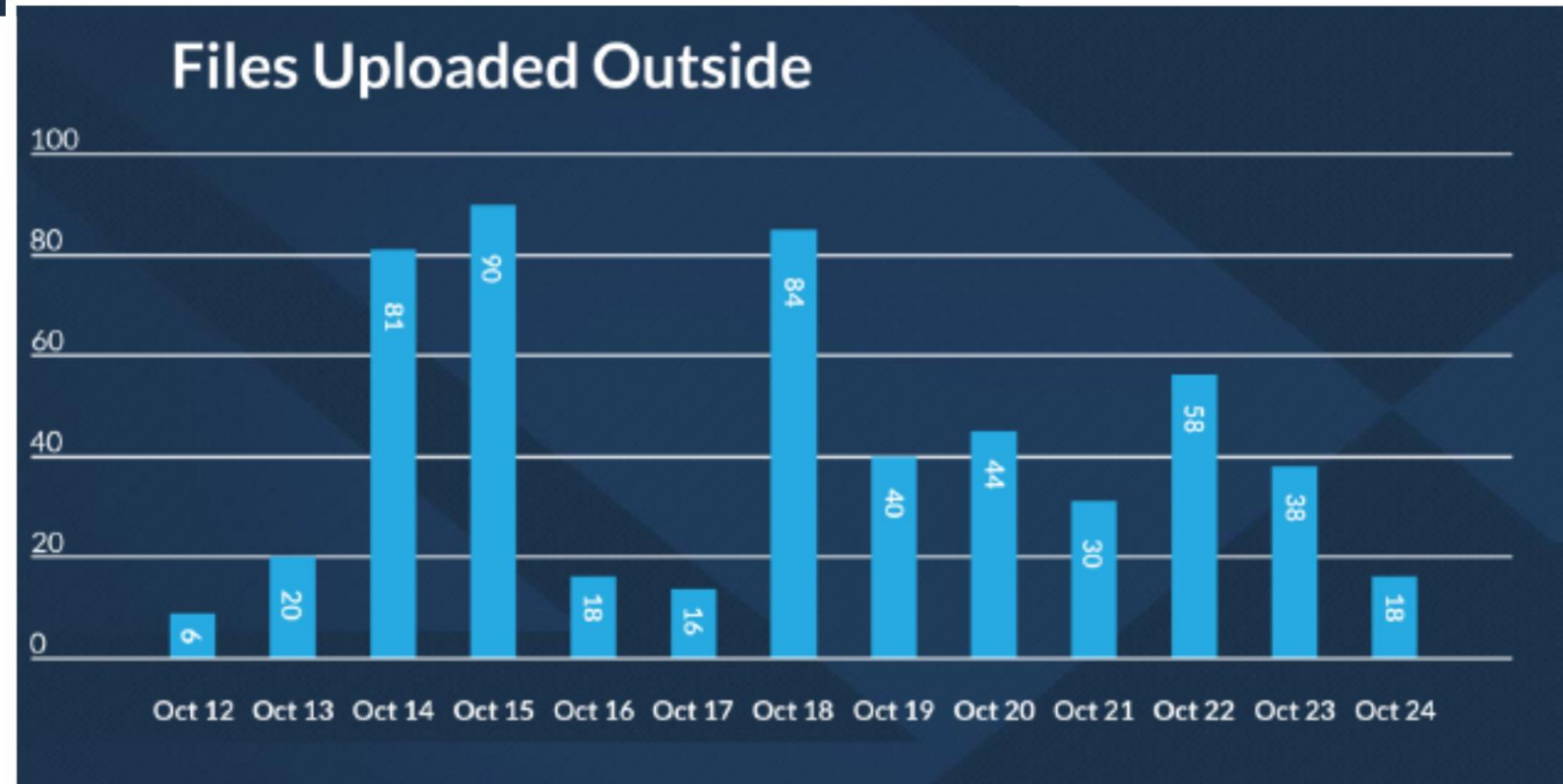
Zmapujte pohyb osobních dat

Tato analýza identifikuje jak se GDPR data pohybují uvnitř Vaší organizace a jakými cestami Vaši organizaci opouštějí. Naše platforma používá stejné datové vzory jako při analýze statických dat a to za účelem identifikace:

Všech typů osobních dat v pohybu

- Úrovní citlivostí těchto dat v pohybu
- Zdroj a cíl, tedy odkud a kam jsou osobní data přenášena
- Kanály, kterými osobní data opouštějí Vaši organizaci, např. web, email….


1,000
100
10
1
Total Files
Total MB
294
742
82
197
54
936
75
184
9
25
0.16
3
evernote.com
dropbox.com
store.hightail.com
storage.live.com
kobelco.egnyte.com
drive.google.com


Files Uploaded Outside
100
80
60
40
20
0
6
20
81
90
18
16
84
40
44
30
58
38
18
Oct 12
Oct 13
Oct 14
Oct 15
Oct 16
Oct 17
Oct 18
Oct 19
Oct 20
Oct 21
Oct 22
Oct 23
Oct 24

Fáze 3 - Report a doporučení

Připravte se na nápravná opatření
Jakmile jsou obě analýzy (statická data a data v pohybu) dokončeny, poskytne Vám Atos náhled na Vaše GDPR data který potřebujete k rozhodnutí, kde jsou rizika největší a jaké by měly být Vaše další kroky. Tento náhled ve formě reportu v sobě zahrnuje:

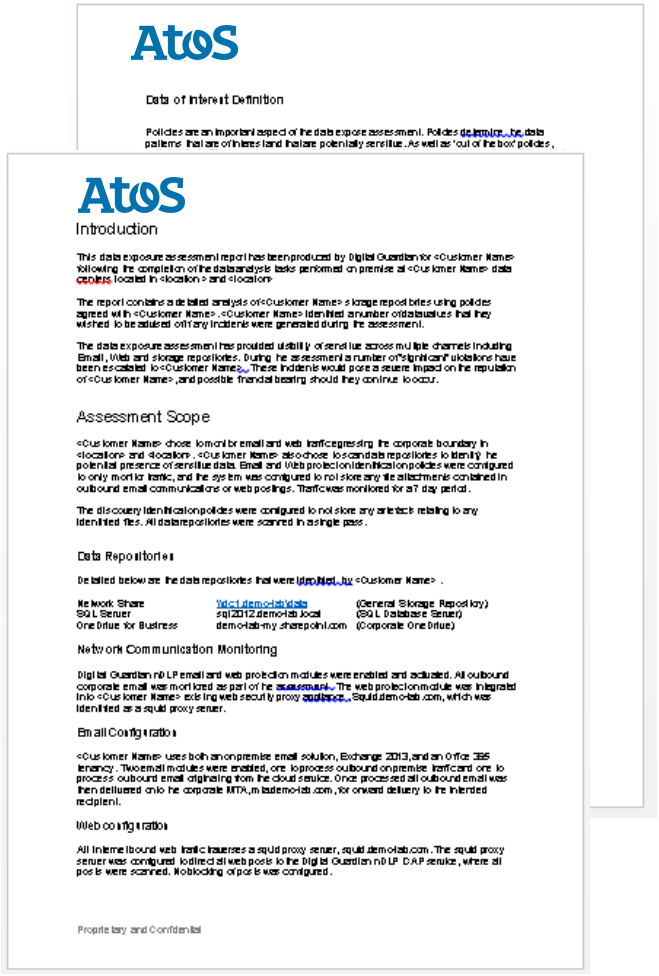
- Ucelený přehled rizik
- Detailní report analýzy dat
- Přehled zjištění
- Doporučení strategie nápravných opatření

4

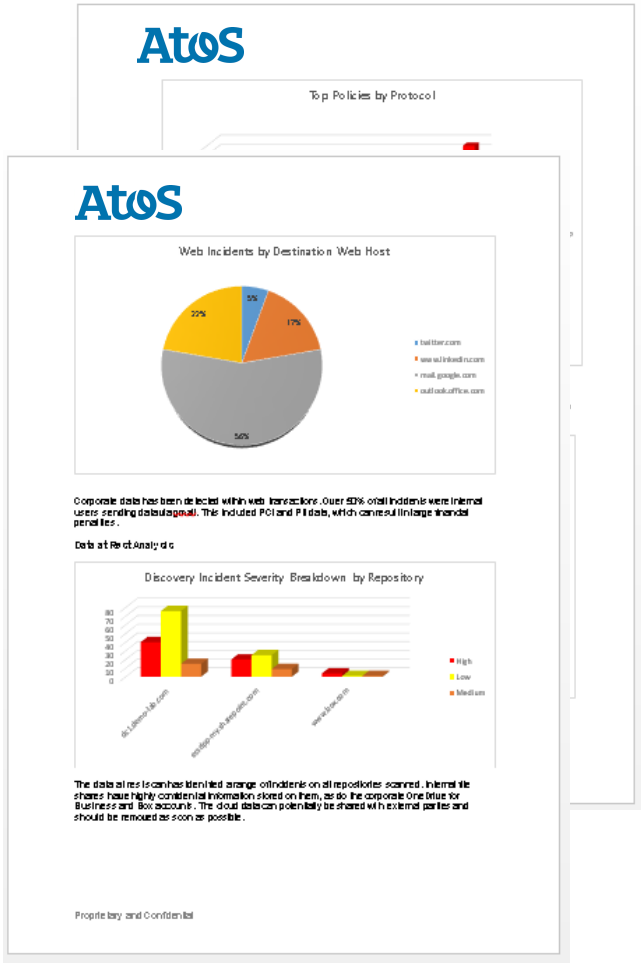
Report a návrh nápravných opatření

Fáze 3 - Report

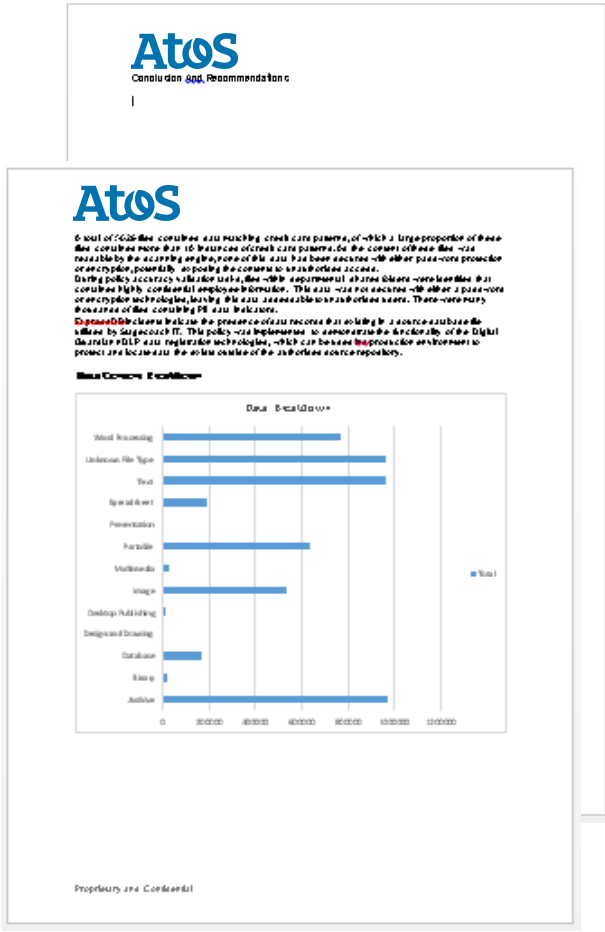
Detailní popisy



Datový audit



Doporučení



5 základních otázek – pamatujete?

Otázka	Výstup v reportu
1. Jaká osobní data občanů EU máte v držení?	Detailní popis, kde se data obsahující osobní údaje nacházejí vč. rozložení po jednotlivých zdrojích.
2. Jak citlivá data to jsou?	Popis způsobů vč. četnosti, jak osobní údaje opouštějí Vaši organizaci.
3. Kde přesně v rámci organizace se tato nacházejí?	Detailní popis úložišť obsahujících osobní data.
4. Jak se v rámci organizace pohybují a kam a jakými kanály z organizace odcházejí?	Real-time a historický pohled na osobní data opouštějící Vaši organizaci umožní detekovat a notifikovat o potenciálním úniku osobních dat.
5. Jak se s nimi pracuje a komu jsou poskytována?	Doporučení politik, architektury a životního cyklu dokumentů k zajištění vyšší úrovně ochrany.

5 Zavádění nápravných opatření

Management summary nápravných opatření

ID	Popis problému	Úroveň rizika	Opatrenia	Doba realizácie (týždne/Mesiace)	Náklady na implementáciu opatrenia (MD/ Eur bez DPH)	Ročné náklady na správu implementovaného opatrenia (MD / Eur bez DPH)	Priorita riešenia (1/2/3)*
ID6	Nie sú jasne identifikované všetky osobné údaje, informačné systémy osobných údajov, spracovateľské operácie s osobnými údajmi ani subjekty, ktoré sa podieľajú na spracúvaní osobných údajov.	Vysoká	A) Vykonať audit spracúvania osobných údajov. A) Identifikovať všetky spracovateľské operácie s osobnými údajmi. A) Identifikovať všetky systémy osobných údajov. A) Identifikovať všetkých sprostredkovateľov. A) Identifikovať všetkých zamestnancov prichádzajúcich do styku s osobnými údajmi.	1-2 Mes.	100 MD	20 MD	1
ID18	Na PCs, notebookoch a serveroch nie je kontrolované, ktoré údaje odchádzajú/prichádzdajú z/na koncových zariadení.	Kritická	A) Zadefinovať citlivé dáta, ktoré majú byť chránené. B) Zaviesť pravidlá na ochranu pred únikom citlivých dát. C) Implementovať nástroje a bezpečnostné mechanizmy slúžiace na ochranu úniku citlivých a dôverných informácií prostredníctvom elektronickej pošty, internetu, FTP komunikácie a využitím USB, Bluetooth a pod. rozhraní – implementovať DLP (Data Leak Prevention systému).	1,5Mes – 4Mes.	50 MD SW/HW: 150-200 tis. Eur	50 MD	1

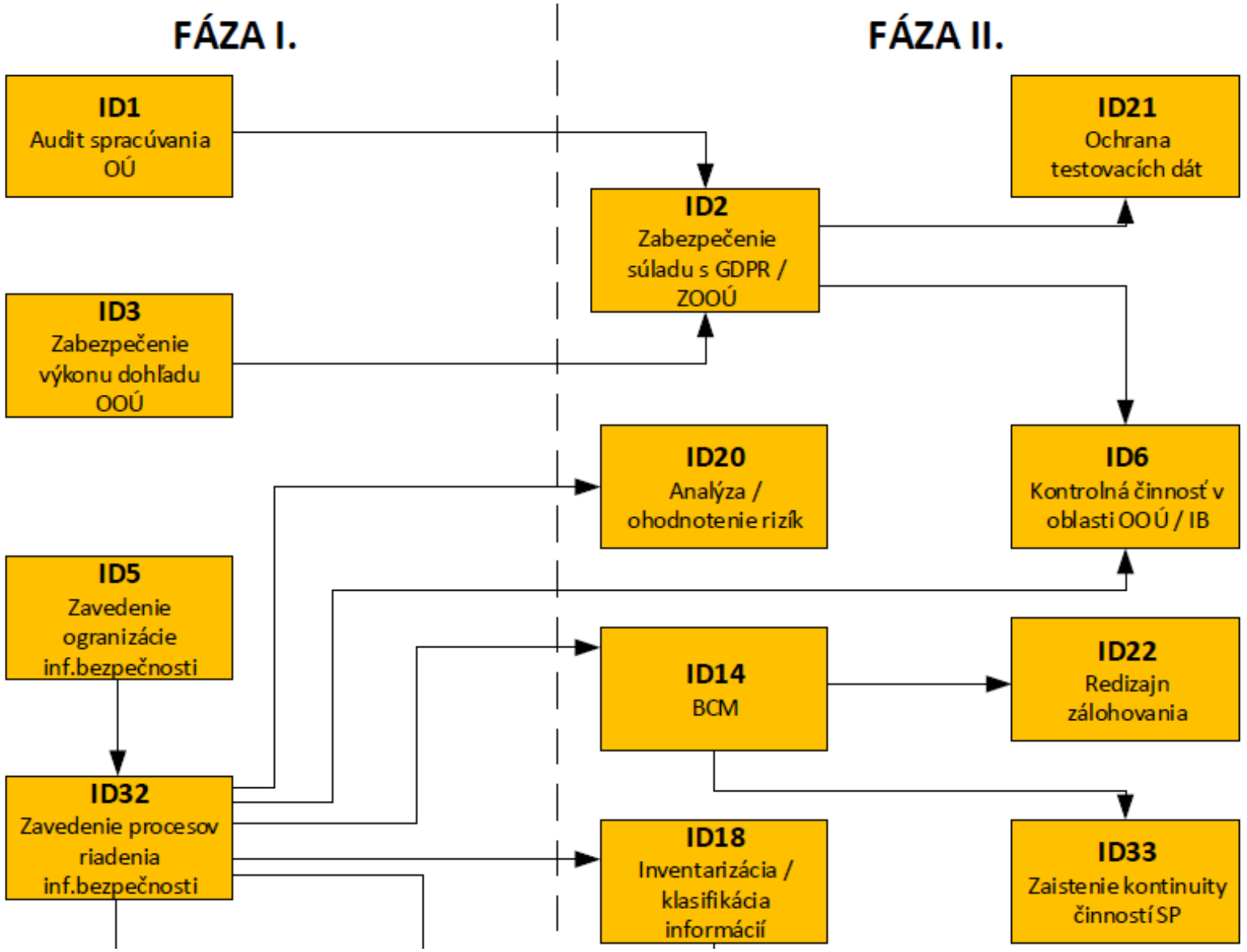
Technické a procesní specifikace coby podklad pro realizaci nápravných opatření

Technická špecifikácia:

Minimální požadavky na dodávané řešení jsou následující:

Parameter	Minimálna požiadavka obstarávateľa
NetFlow Sonda	
Pasívne zapojenie	Pasívne zapojenie bez vplyvu na monitorovanie sieť (SPAN / mirror portami) pre každú lokalitu
Inštalácia	HW, Racková montáž
Management rozhranie	2 x (administratívne) porty 10/100 / 1000Mb / s (UTP kabeláž) pre zabezpečenú vzdialenú správu a prenos NetFlow dát,zabezpečená vzdialená správa, dohľad a konfigurácia - SSH, HTTPS.
Správa užívateľov a prístupových práv	Správa užívateľov a prístupových práv na zariadení prostredníctvom užívateľských rolí.
Nastaviteľná rýchlosť monitorovacej linky	2x 10 Gb / s na optickom rozhraní (2x 10G-SFP-SR)
Vstavaný kolektor	Vstavaný kolektor pre dočasné ukladanie flow štatistík (zaistenie redundancie) min o kapacite 0,5 TB
Časová synchronizácia	Časová synchronizácia zariadenia proti centrálnemu zdroju času na sieti.

Roadmap nápravných opatření



Součástí reportu je i kvantifikace nápravných opatření a návrh jejich rozložení v čase podle časových, finančních možností zákazníka.

ATOS program ochrany GDPR dat

Poznejte, kde máte uložena osobní data, jak je s nimi nakládáno, která data jsou ta nejcitlivější a požadujete pro ně vyšší ochranu.

Zautomatizujte klasifikaci Vašich osobních dat s důrazem na zdroje a jejich kontrolu

Používejte technologie jako je DLP, Identity Acess Management a šifrování

Zaktualizujte si své plány zvládání detekovaných incidentů abyste byli na podobné situace připraveni

Použijte své analýzy a jejich výstupy k předvedení svého souladu s požadavky GDPR

Trusted partner for your Digital Journey