WebArat

pravidlá vo vaších rukách

Komplexný systém riadenia procesov kybernetickej bezpečnosti a GDPR

O systéme WebArat

- WebArat - nástroj pre evidenciu a riadenie oblastí kybernetickej bezpečnosti v logike a súlade ako to navrhuje a požaduje:
  - **ISO 27001**
  - **Zákon o kybernetickej bezpečnosti a súvisiace vyhlášky**
  - a hlavne **Best practice**
- Súčasťou systému je samostatný modul GDPR integrovaný do celkového riadenia kybernetickej bezpečnosti.

*Systém **WebArat** Vám ponúka možnosť mať prehľad a poznať súvislosti a na základe toho riadiť kybernetickú bezpečnosť a GDPR ako celok.*

Pro koho je WebArat určený

- Primárne je určený pre **Manažéra kybernetickej bezpečnosti**
- Sekundárne pre:
  - Garantov primárnych a podporných aktív
  - Vedenie organizácie
  - Audítorov kybernetickej bezpečnosti
  - Správcov dokumentácie
  - DPO

.

Oblasti riadenia v systéme WebArat

Primárne oblasti riadenia

Ciele kybernetickej bezpečnosti
- Plány plnenia cieľov

Informačné aktíva
- Primárne aktíva (informácie, dáta, ...)
- Podporné aktíva (HW, SW, ľudia, ...)

Bezpečnostné opatrenia

Hrozby / zraniteľnosti
- Katalóg hrozieb
- Katalóg zraniteľností

Tretie strany

Analýza rizík
- Plány zvládania rizík
- Riziká
- Rizikové kombinácie

Rizikové scenáre
- Definované hrozby
- Súvisiace zraniteľnosti
- Vybrané primárne aktíva
- Súvisiace podporné aktíva
- Súvisiace bezpečnostné opatrenia

Sekundárne oblasti riadenia

Incident / udalosť
- Incident / udalosť (evidencia)
- Plán zvládania incidentu / udalosti

Audity
- Auditné zistenia
- Zvládanie auditného zistenia (úlohy)

Kontrola
- Kontrolné zistenia
- Zvládanie kontrolného zistenia (úlohy)

Oblasti riadenia v systéme WebArat

Podporné oblasti riadenia

Spoločnosť
- Evidencia zamestnancov
- Role
- Personálne skupiny rolí
- Organizačné úseky
- Pozície
- Budovy

Dokumentácia
- Kompletná dokumentácia
- Tvorba / evidencia dokumentácie
- Pripomienkovanie
- Schvaľovanie
- Evidencia zmien
- Školenie a vzdelávanie

GDRP
- Účely spracovania
- Evidencia súhlasov
- Evidencia žiadostí
- Poučenia a zmluvy
- Posúdenie rizikovosti / vplyvu
- Výstupy GDPR

Výstupy
- OLAP pohľady
- Vlastné výstupy (tabuľky)
- Vlastné grafy

Prehlásenie o aplikovateľnosti

Úkolovník

Pracovné postupy (Workflow)

Upozornenia

Logy

Systémové role

Možnosti implementácie systému WebArat

Alternatíva 1

- implementácia súčasného stavu, metodík a postupov **bez našich doporučení**

Alternatíva 2

- implementácia a **optimalizácia súčasných postupov** (súčasné procesy prejdú revíziou zo strany audítora a architekta kybernetickej bezpečnosti a na základe doporučení budú upravené)

Alternatíva 3

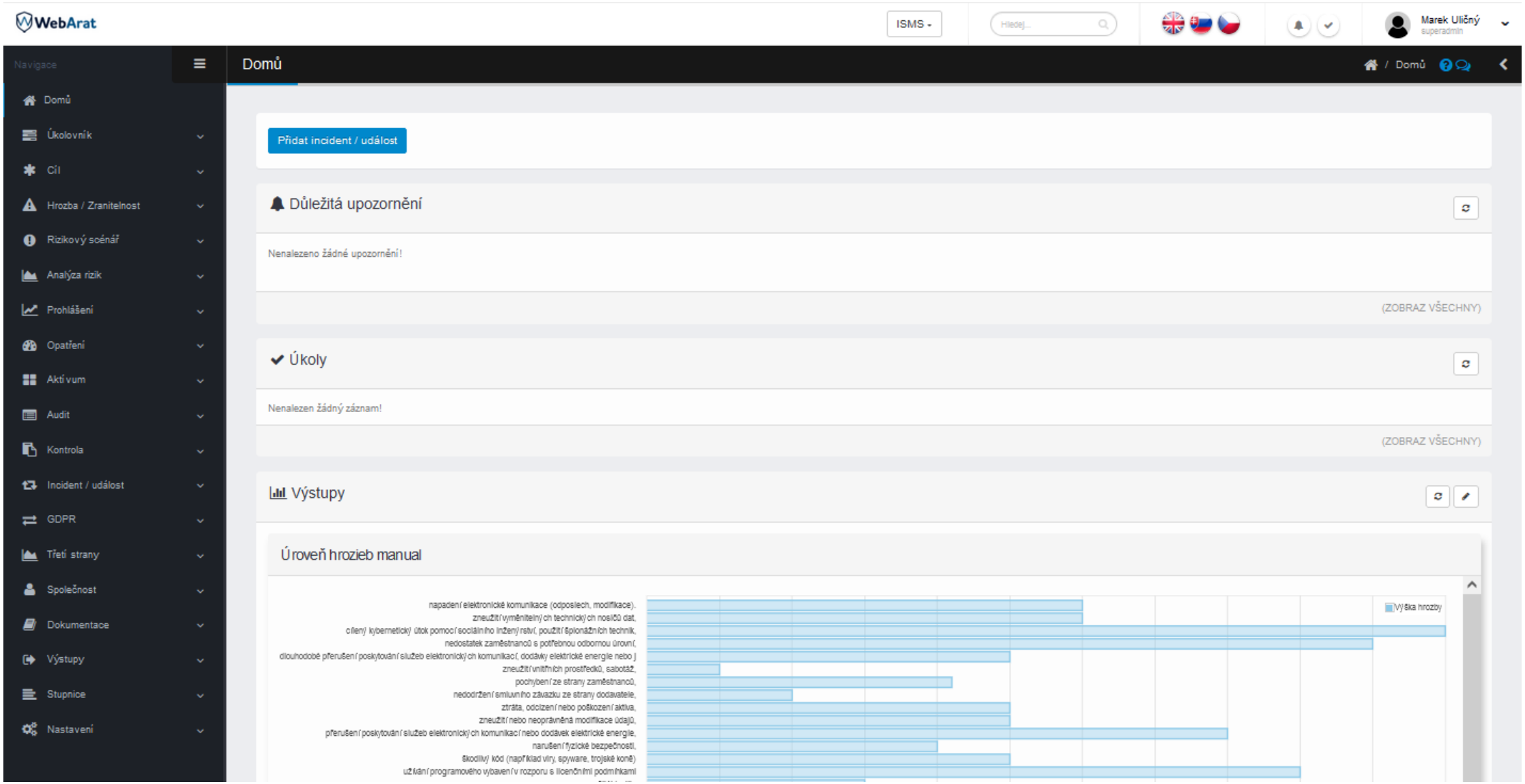
- implementácia **celého systému riadenia kybernetickej bezpečnosti** (identifikácia a vyhodnotenie aktív, analýz rizík, spracovanie bezpečnostnej dokumentácie, bezpečnostných procesov apod.)

Možnosti nasadenia

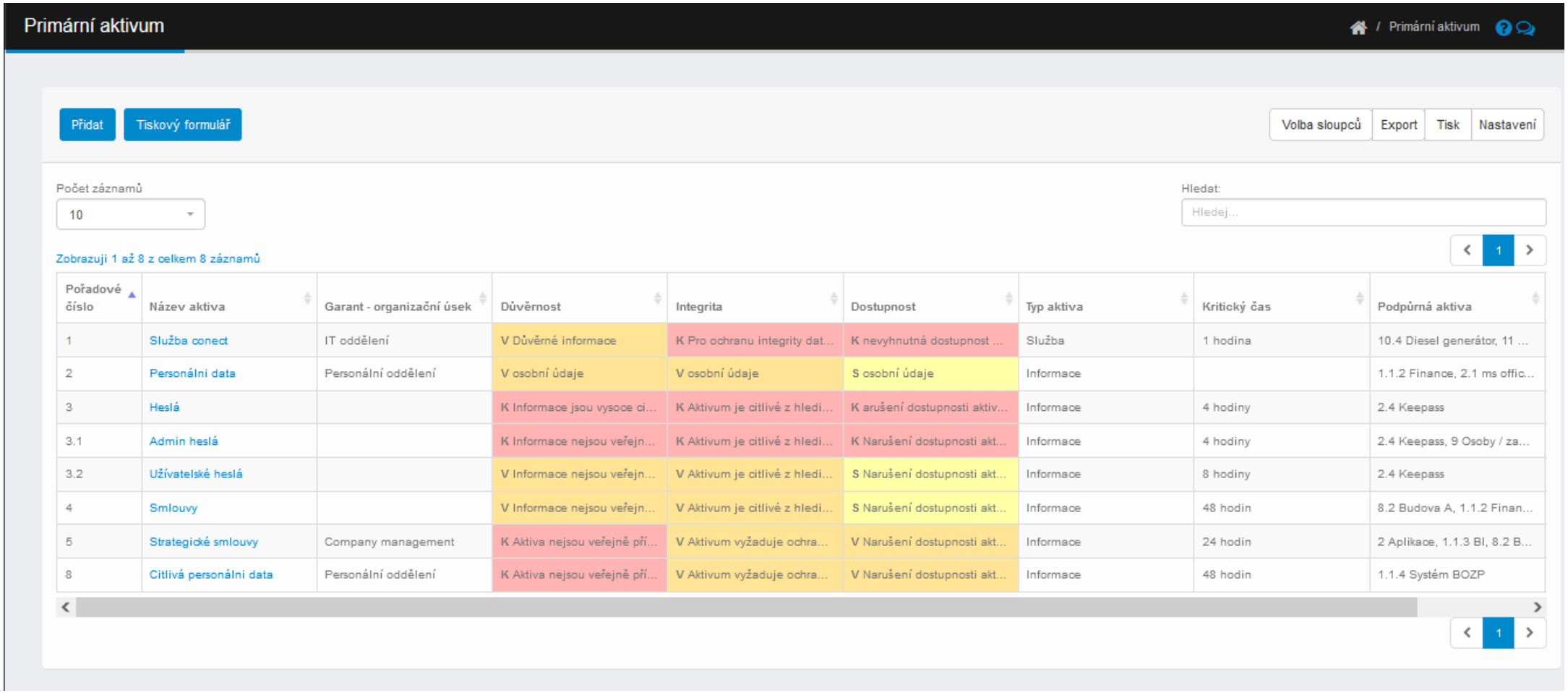
- WebArat je určený pre všetky typy organizácií a rôzne štruktúry riadenia
  - Základná – Manažér KB, ktorý má WebArat nasadený vo svojom pc /notebooku a kompletnú evidenciu a záznamy si riadi sám
  - Rozšírená - systém je nasadený v organizácii a pripája sa k nemu len úzky okruh kompetentných osôb
  - Kompletná - systém je nasadený v organizácii a pripájajú sa k nemu všetci zamestnanci, garanti aktív, riadiaci pracovníci a tiež zamestnanci, ktorí majú plniť jednotlivé úlohy, vzdelávajú sa, pripomienkujú alebo schvaľujú dokumentáciu, …
- Možnosti nasadenia
  - On premise (doporučené pro rozšírené a kompletné nasadenie)
  - SaaS

Vybrané ukážky prostredia systému WebArat

Prostredie systému WebArat

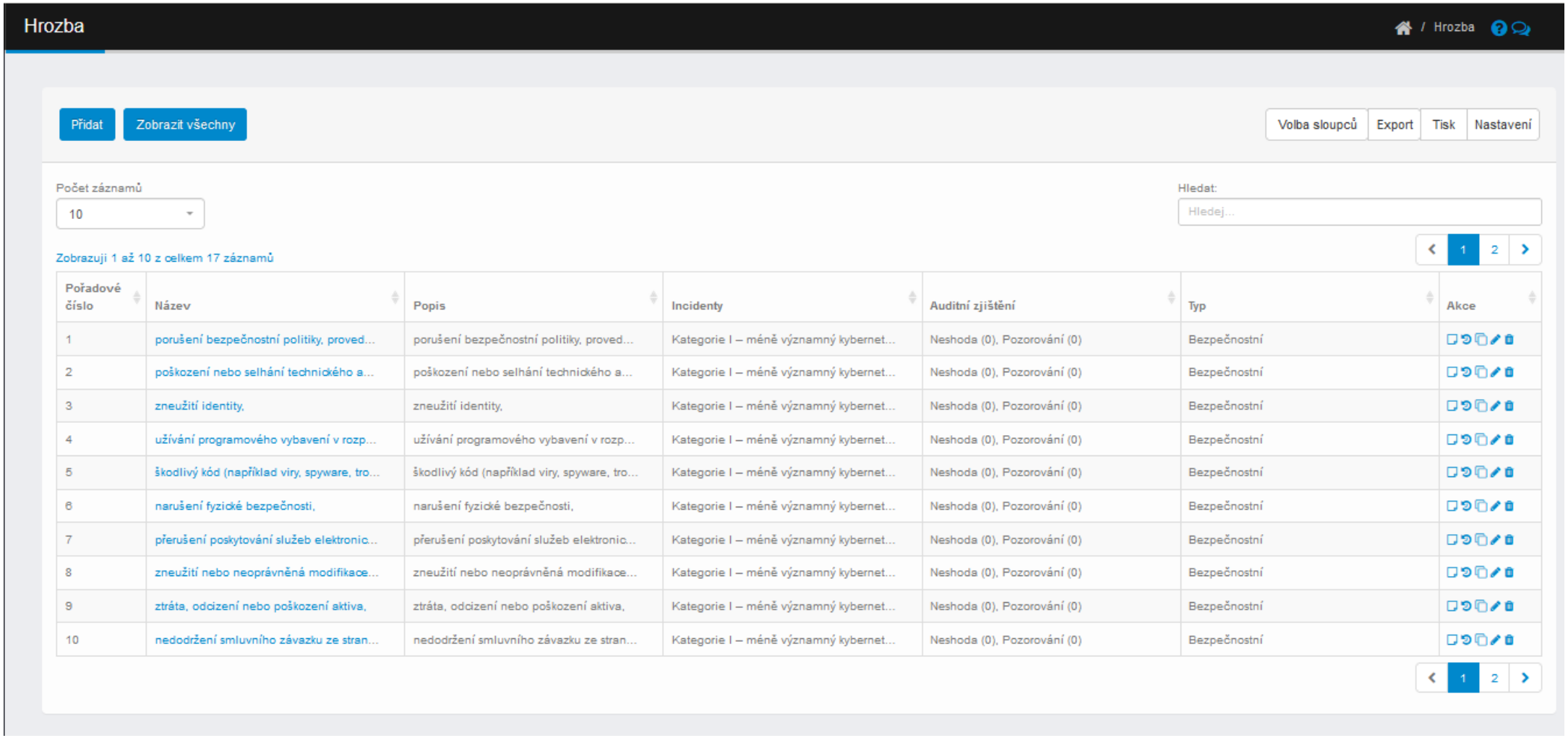


Katalóg primárnych aktív

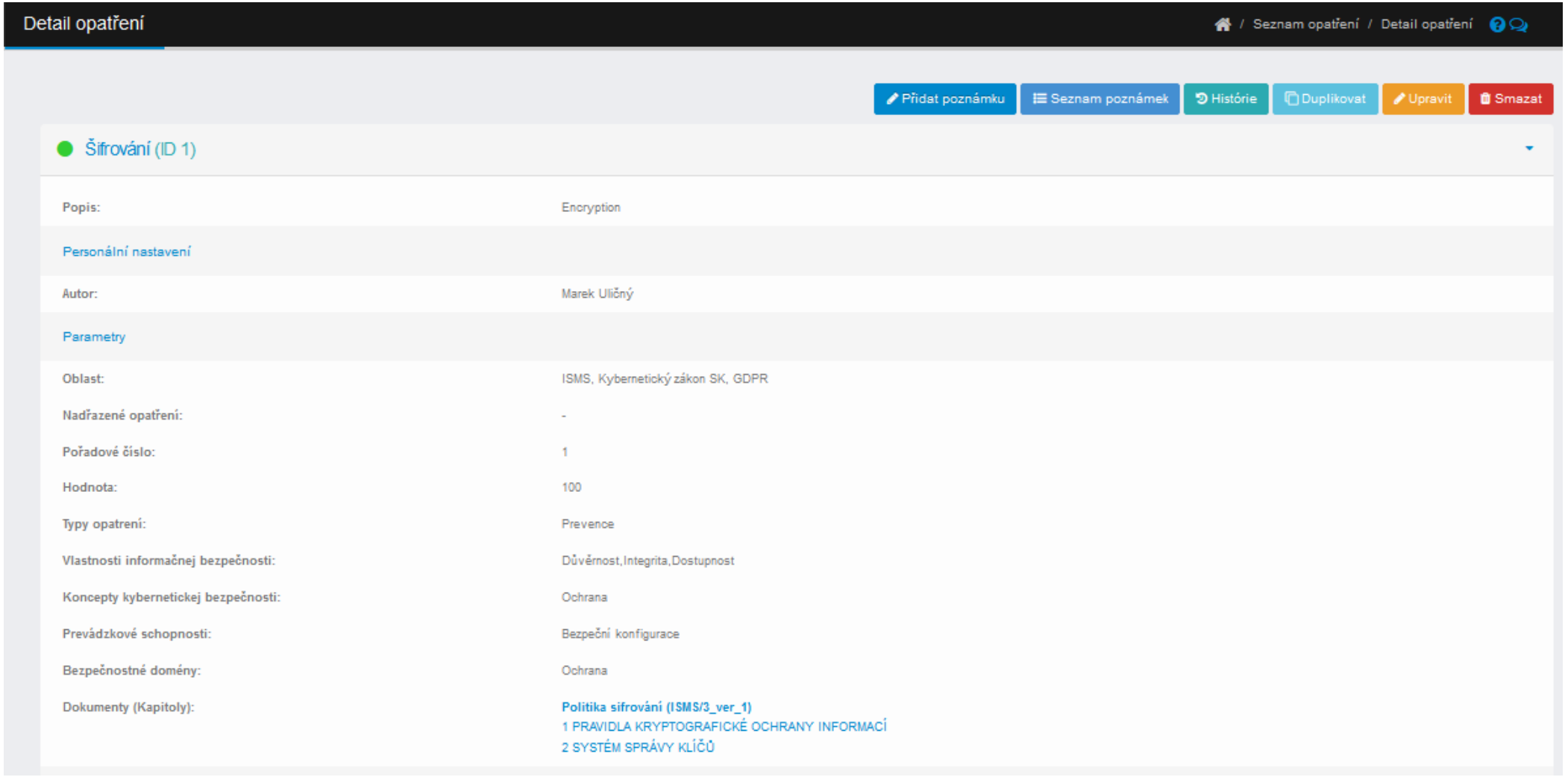


WebArat

Katalog hrozieb

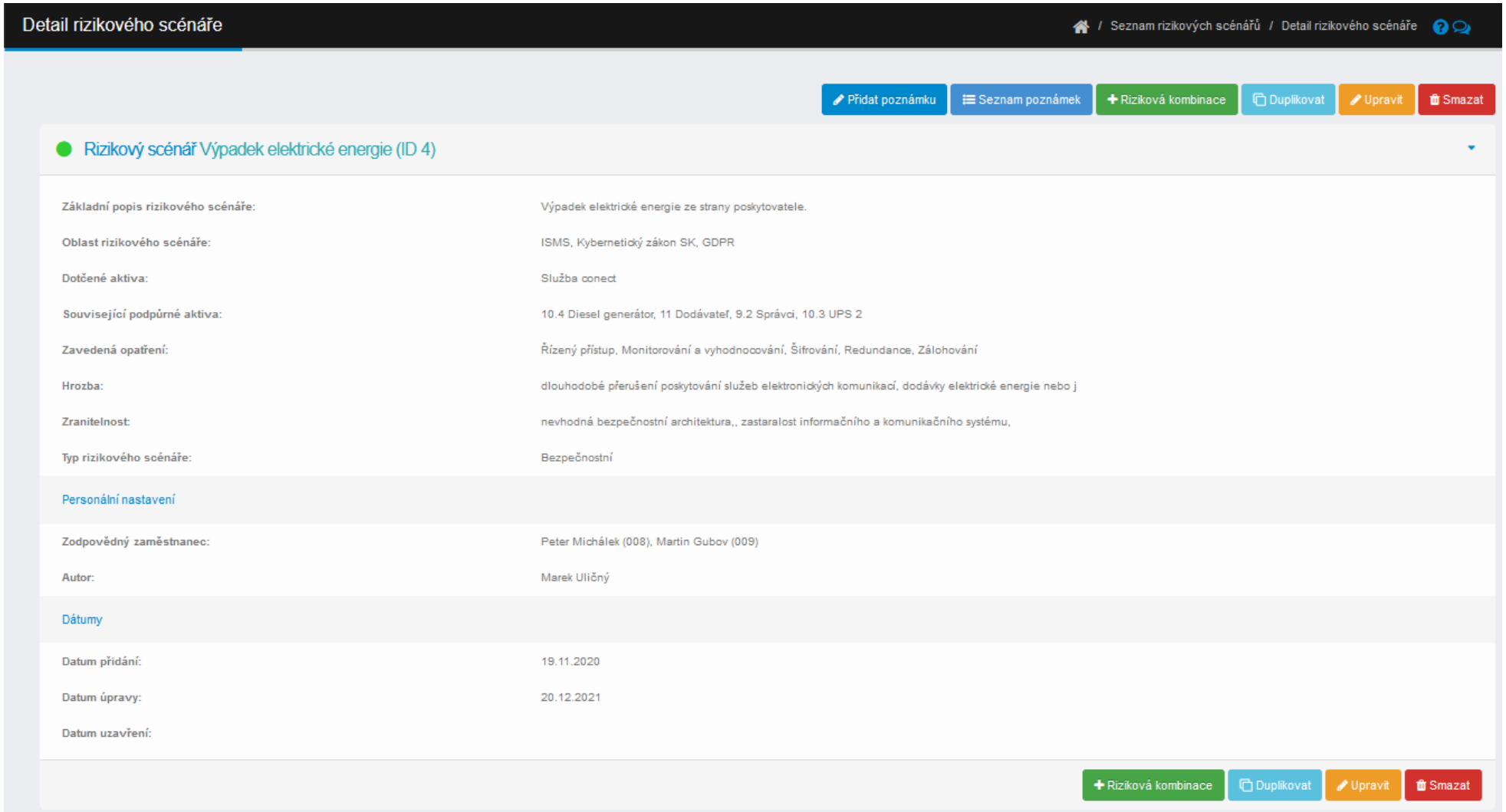


Opatrenia - detail



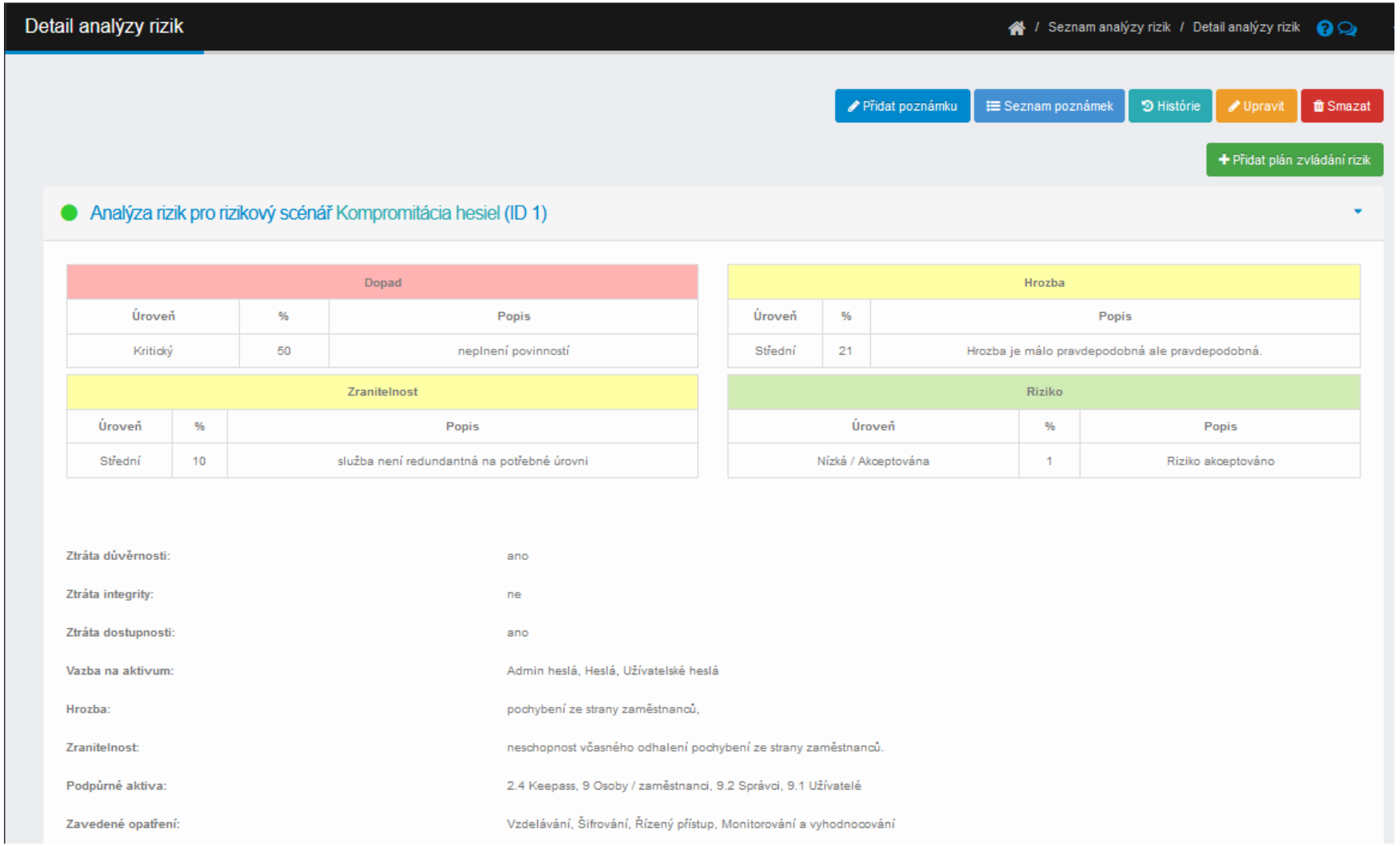
WebArat

Rizikové scenáre - detail



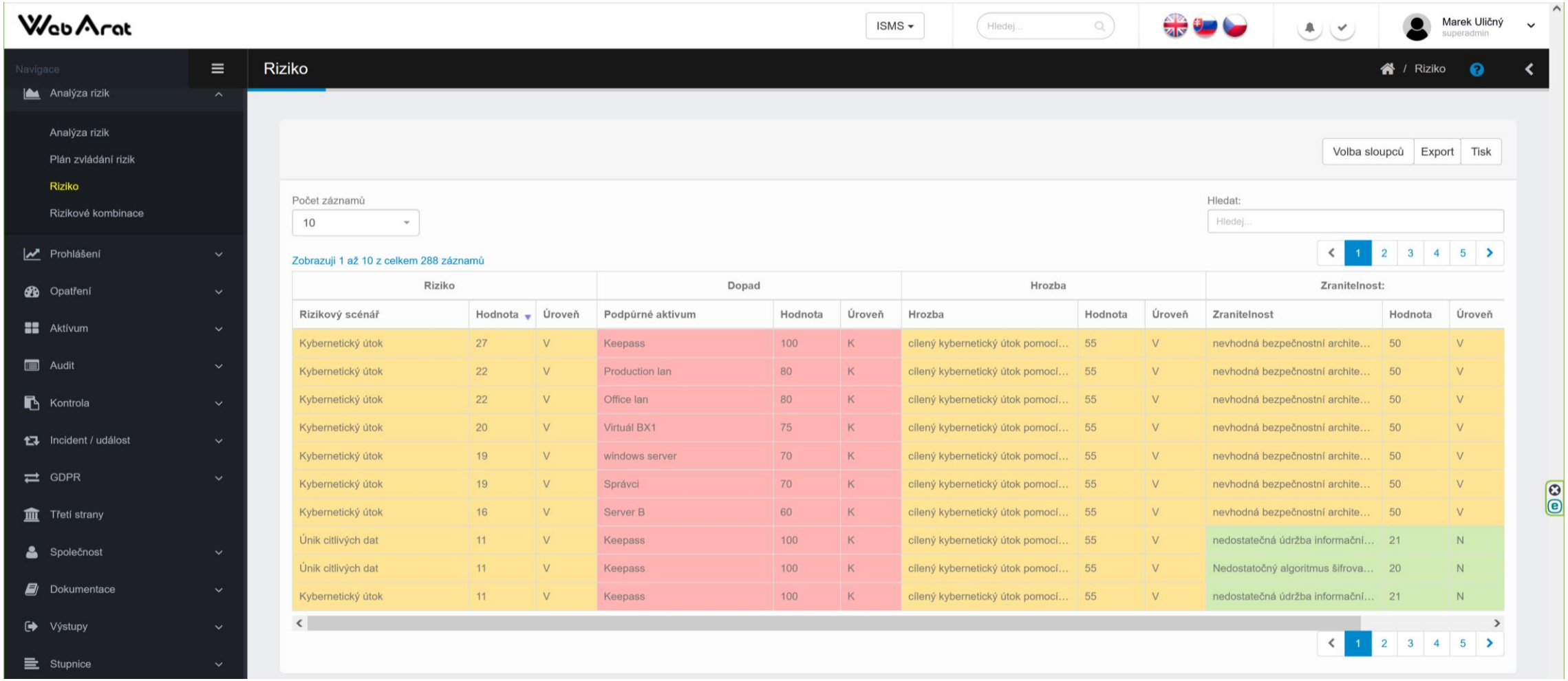
WebArat

Vyhodnotenie rizika - detail

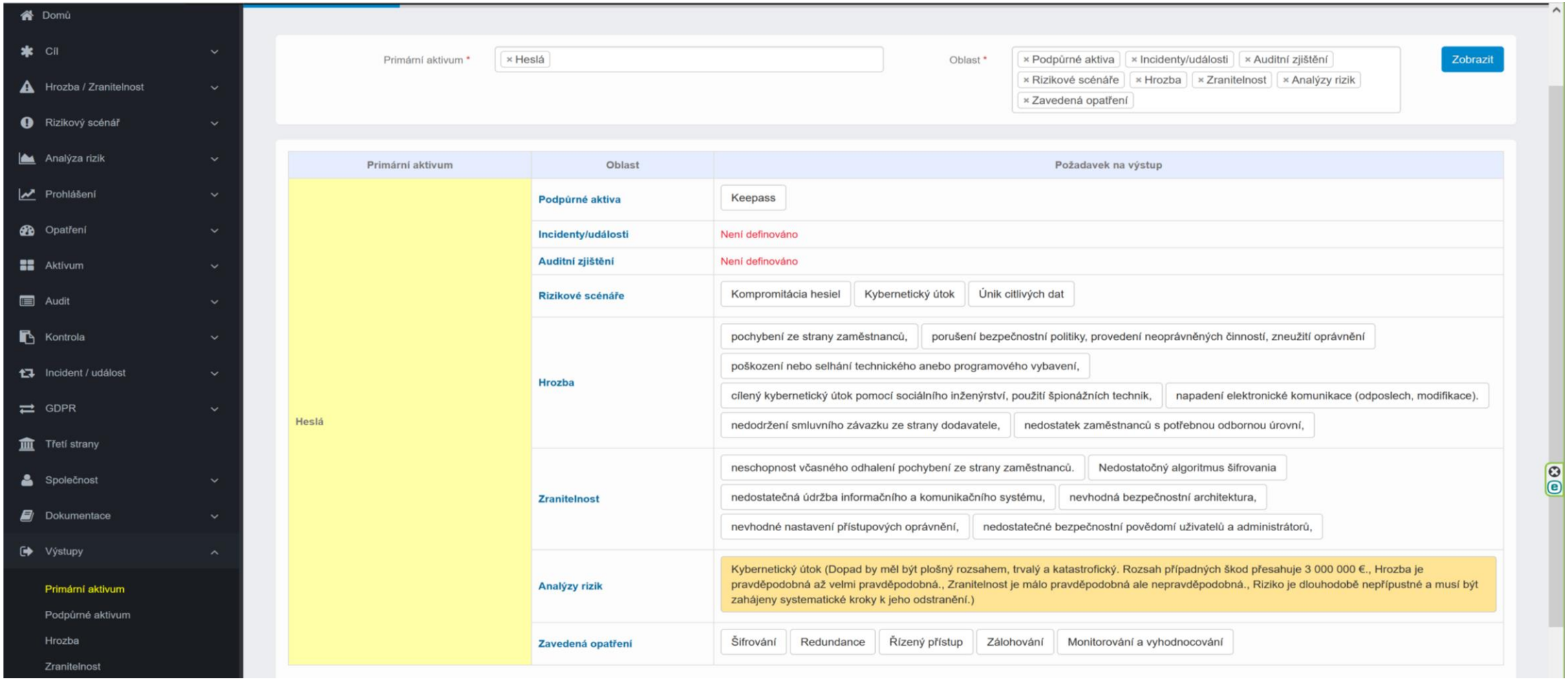


WebArat

Rizikovosť


WebArat
ISMS
Hledej...
Marek Uličný
superadmin
Navigace
Riziko
Riziko
Analýza rizik
Analýza rizik
Plán zvládání rizik
Riziko
Rizikové kombinace
Prohlášení
Opatření
Aktívum
Audit
Kontrola
Incident / událost
GDPR
Třetí strany
Společnost
Dokumentace
Výstupy
Stupnice
Volba sloupců
Export
Tisk
Počet záznamů
10
Hledat:
Hledej...
Zobrazuji 1 až 10 z celkem 288 záznamů
1 2 3 4 5
Riziko
Dopad
Hrozba
Zranitelnost:
Rizikový scénář
Hodnota
Úroveň
Podpůrné aktivum
Hodnota
Úroveň
Hrozba
Hodnota
Úroveň
Zranitelnost
Hodnota
Úroveň
Kybernetický útok 27 V Keepass 100 K cílený kybernetický útok pomocí... 55 V nevhodná bezpečnostní archite... 50 V
Kybernetický útok 22 V Production lan 80 K cílený kybernetický útok pomocí... 55 V nevhodná bezpečnostní archite... 50 V
Kybernetický útok 22 V Office lan 80 K cílený kybernetický útok pomocí... 55 V nevhodná bezpečnostní archite... 50 V
Kybernetický útok 20 V Virtuál BX1 75 K cílený kybernetický útok pomocí... 55 V nevhodná bezpečnostní archite... 50 V
Kybernetický útok 19 V windows server 70 K cílený kybernetický útok pomocí... 55 V nevhodná bezpečnostní archite... 50 V
Kybernetický útok 19 V Správci 70 K cílený kybernetický útok pomocí... 55 V nevhodná bezpečnostní archite... 50 V
Kybernetický útok 16 V Server B 60 K cílený kybernetický útok pomocí... 55 V nevhodná bezpečnostní archite... 50 V
Únik citlivých dat 11 V Keepass 100 K cílený kybernetický útok pomocí... 55 V nedostatečná údržba informační... 21 N
Únik citlivých dat 11 V Keepass 100 K cílený kybernetický útok pomocí... 55 V Nedostatočný algoritmus šifrova... 20 N
Kybernetický útok 11 V Keepass 100 K cílený kybernetický útok pomocí... 55 V nedostatečná údržba informační... 21 N
1 2 3 4 5

Výstupy systému WebArat



Záver

Celkový výsledok práce so systémom WebArat má priniesť prehľad a schopnosť či už preventívne alebo reaktívne reagovať na potenciálne hrozby (a určite i poskytnúť komplexné informácie o riadení pri kontrolách a auditoch KB).

Ďakujem za pozornosť

Ing. Marek Uličný

Slovenská republika:		Česká republika:
WebArat Solutions, s.r.o.	**SophistIT, s.r.o.**	**Alef NULA, a.s.,**
(+421) 948 834 347 webarat@webarat.sk	(+421) 2 20 62 06 70 info@sophistit.com	(+420) 702 259 478 radek.svadlenka@alef.com