

Od rizika k řešení

… praktická ukázka analýzy rizik pomocí CSA

GORDIC v číslech

Česká technologická společnost dlouhodobě zaměřená na veřejnou správu

30+
let zkušeností

400
odborníků

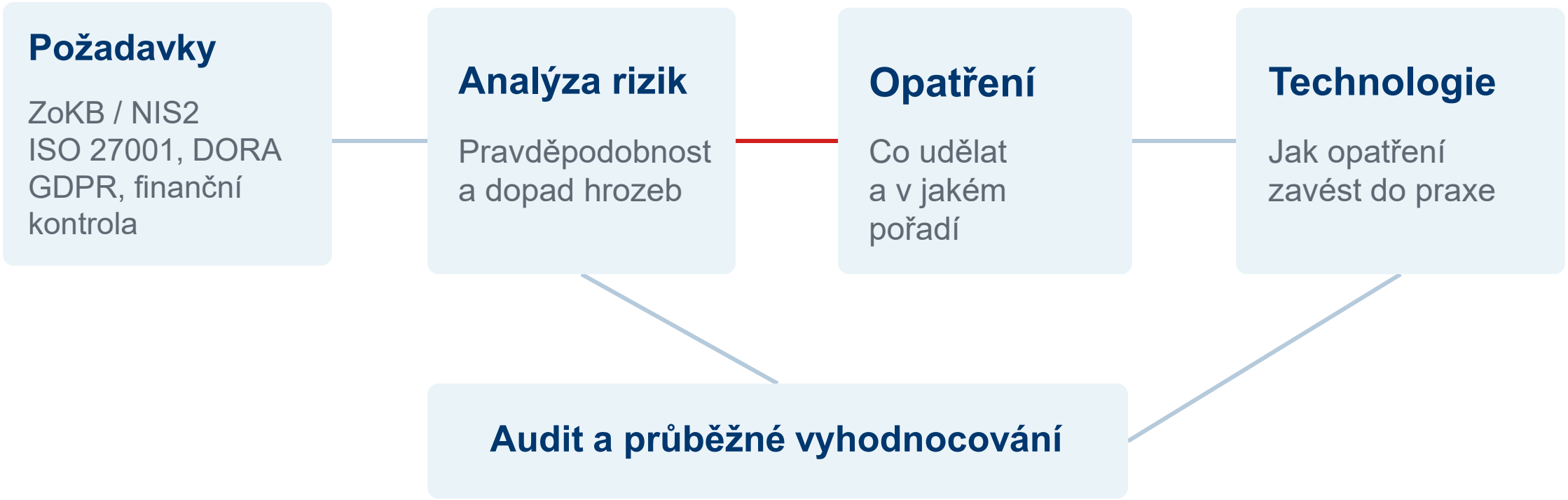
6 000
organizací

150 mil.
dokumentů v systémech

Vlastní vývoj a odborné týmy v ČR.
Dlouhodobá podpora a reakce na legislativní změny.

Nejdříve rizika. Potom opatření.

Analýza rizik určuje priority kyberbezpečnosti.



Intuitivní nástroj pro analýzu rizik



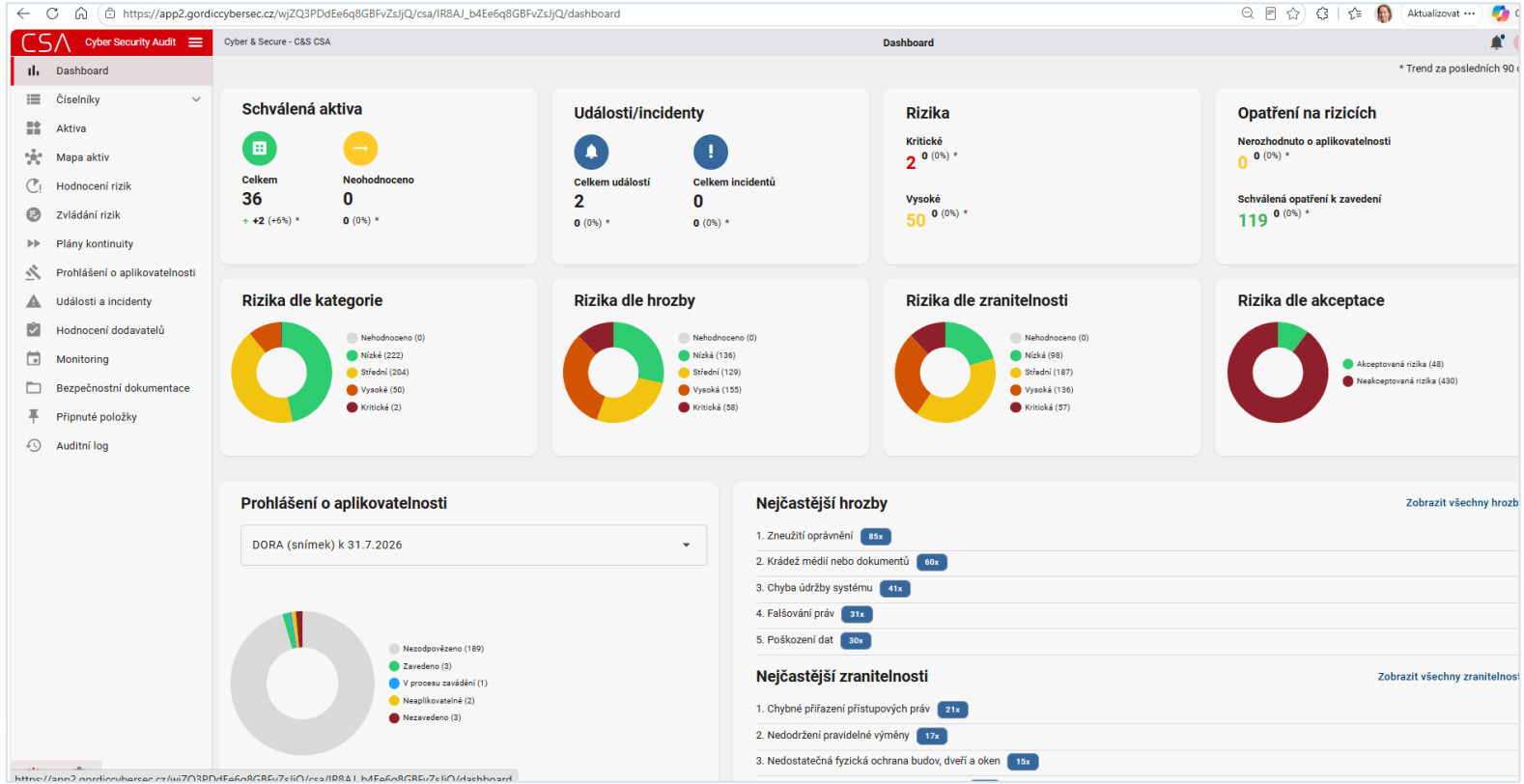
- Evidence aktiv
- Hodnocení aktiv
- Identifikace rizik
- Hodnocení rizik
- Plán zvládání rizik
- Evidence a hodnocení dodavatelů
- Prohlášení o aplikovatelnosti
- Předdefinovaná metodika, typová aktiva
- Přístup na základě rolí a oprávnění

Jedna platforma. Více metodik.



Ukázka – video CSA

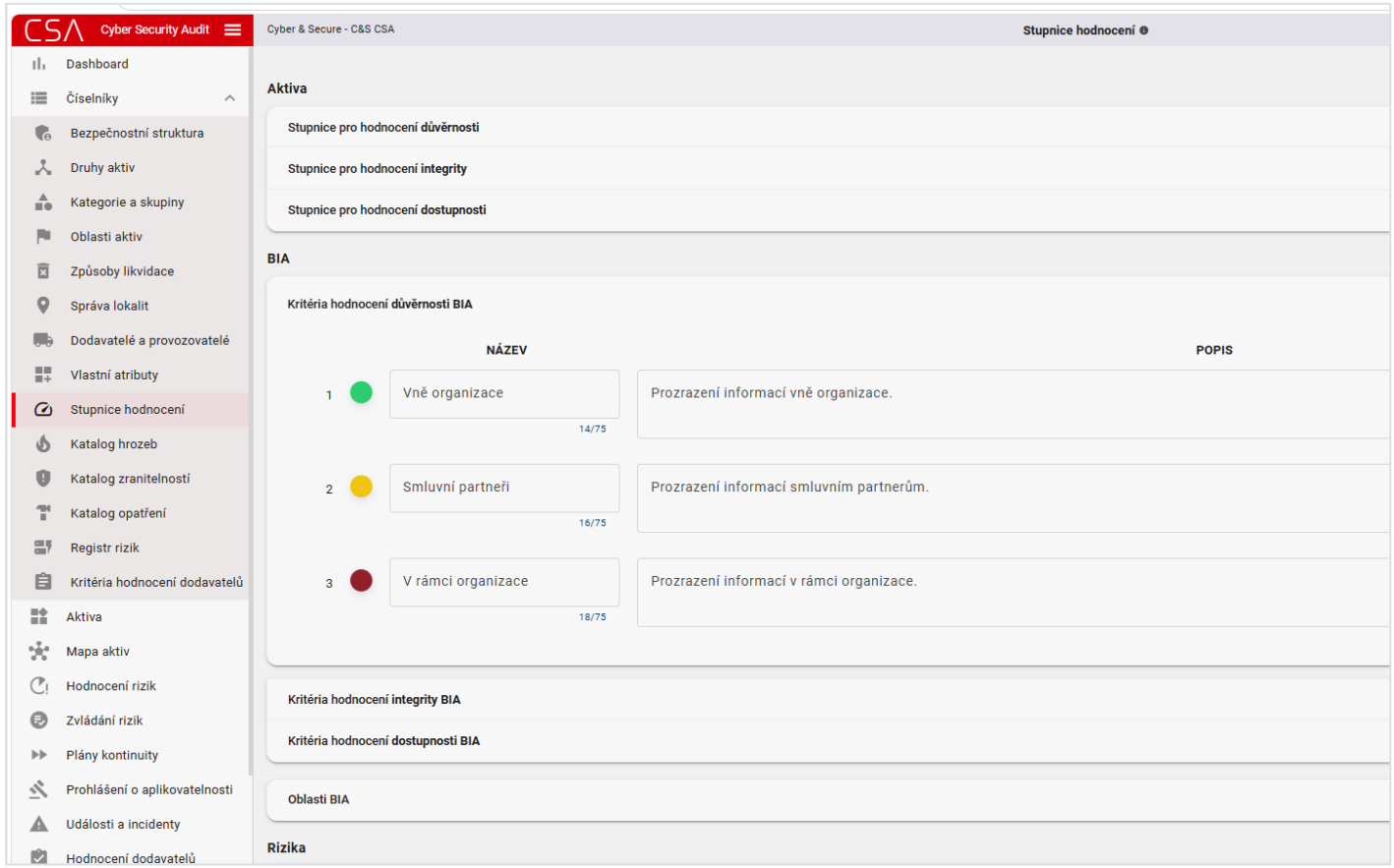
Přehledný dashboard



Co vidíme na první pohled

- Stav analýzy na jednom místě
- Priority pro další rozhodování

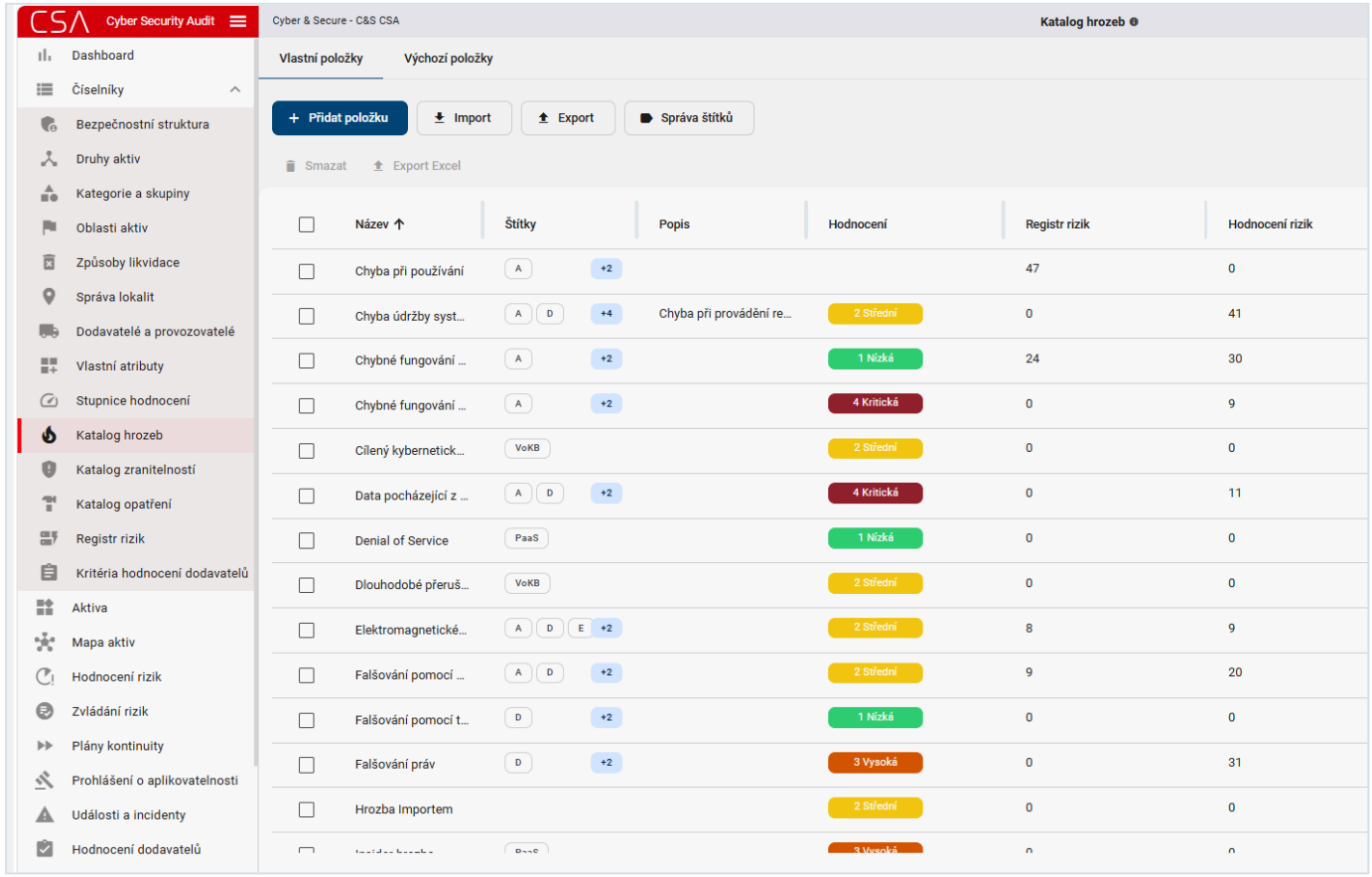
Nastavení číselníků



Nejdřív nastavíme pravidla

- Předdefinovaná metodika
- Úprava stupnic a údajů organizace
- synchronizace uživatelů EntraID, AD

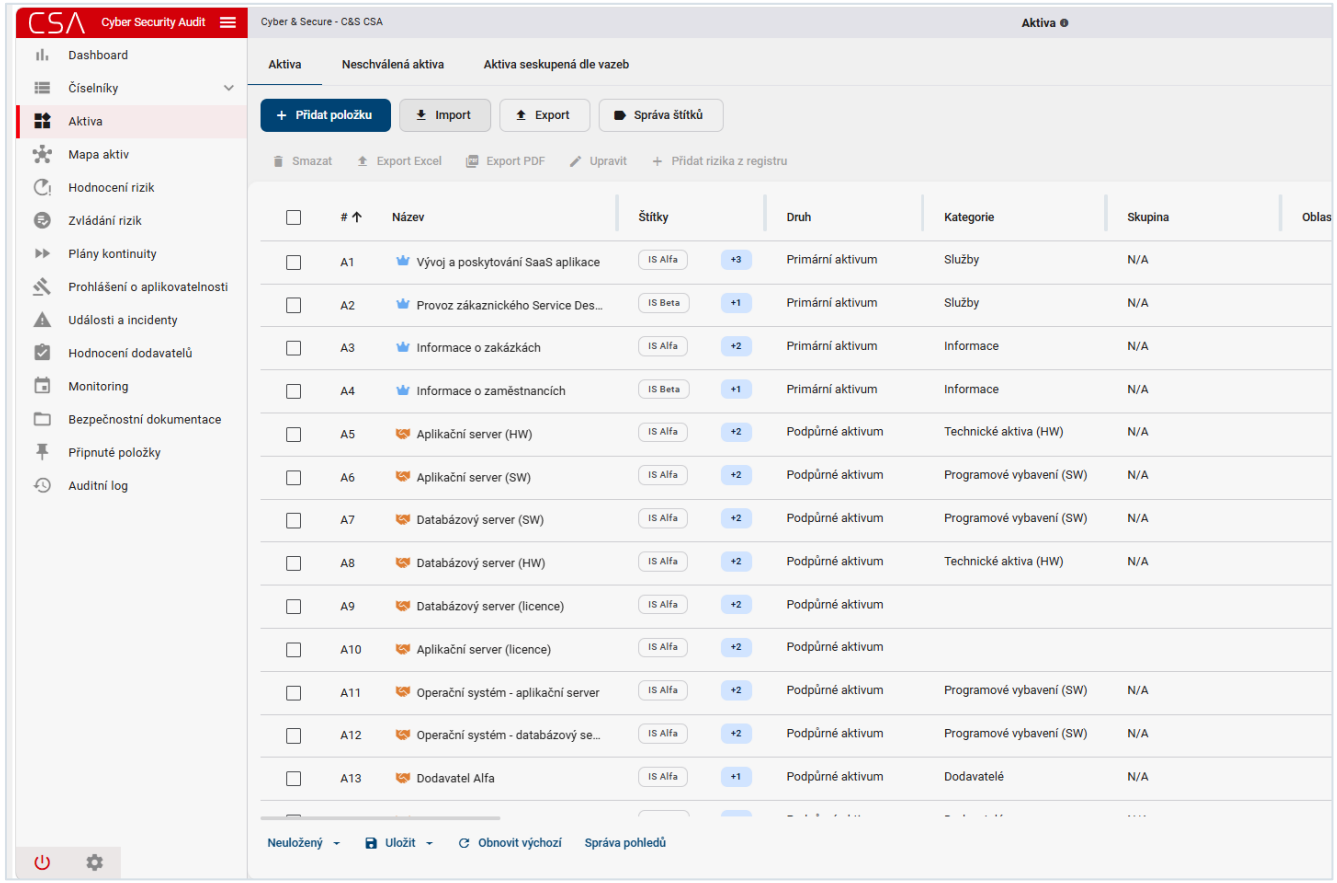
Katalog hrozeb a zranitelností možno předhodnotit



Příprava šetří čas

- Katalog hrozeb a zranitelností
- Předhodnocení pro další práci

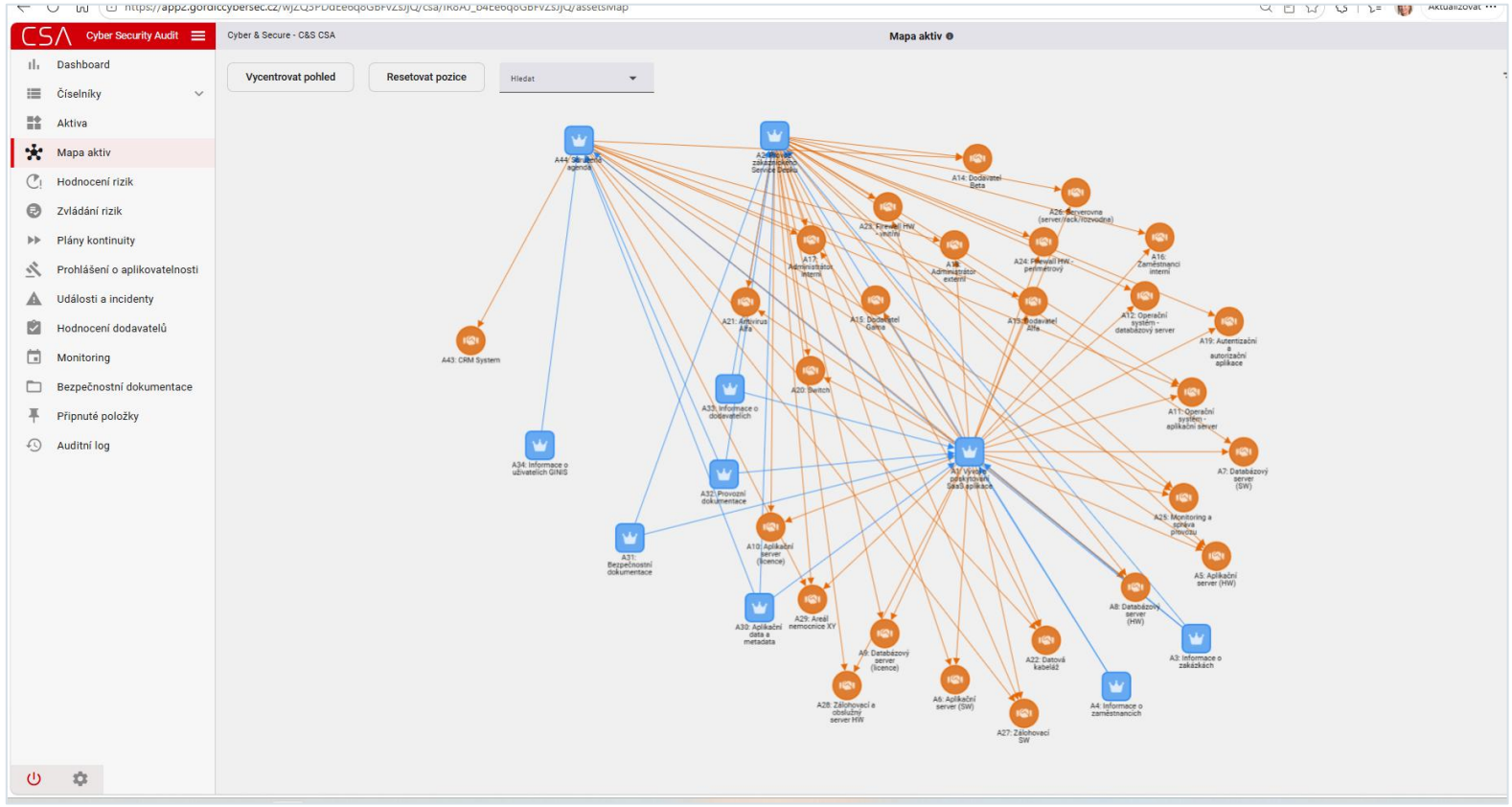
Evidence aktiv



Co vlastně chráníme?

- Evidence a import aktiv (xls, CMDB)
- Vazby mezi aktivy a vlastní filtry

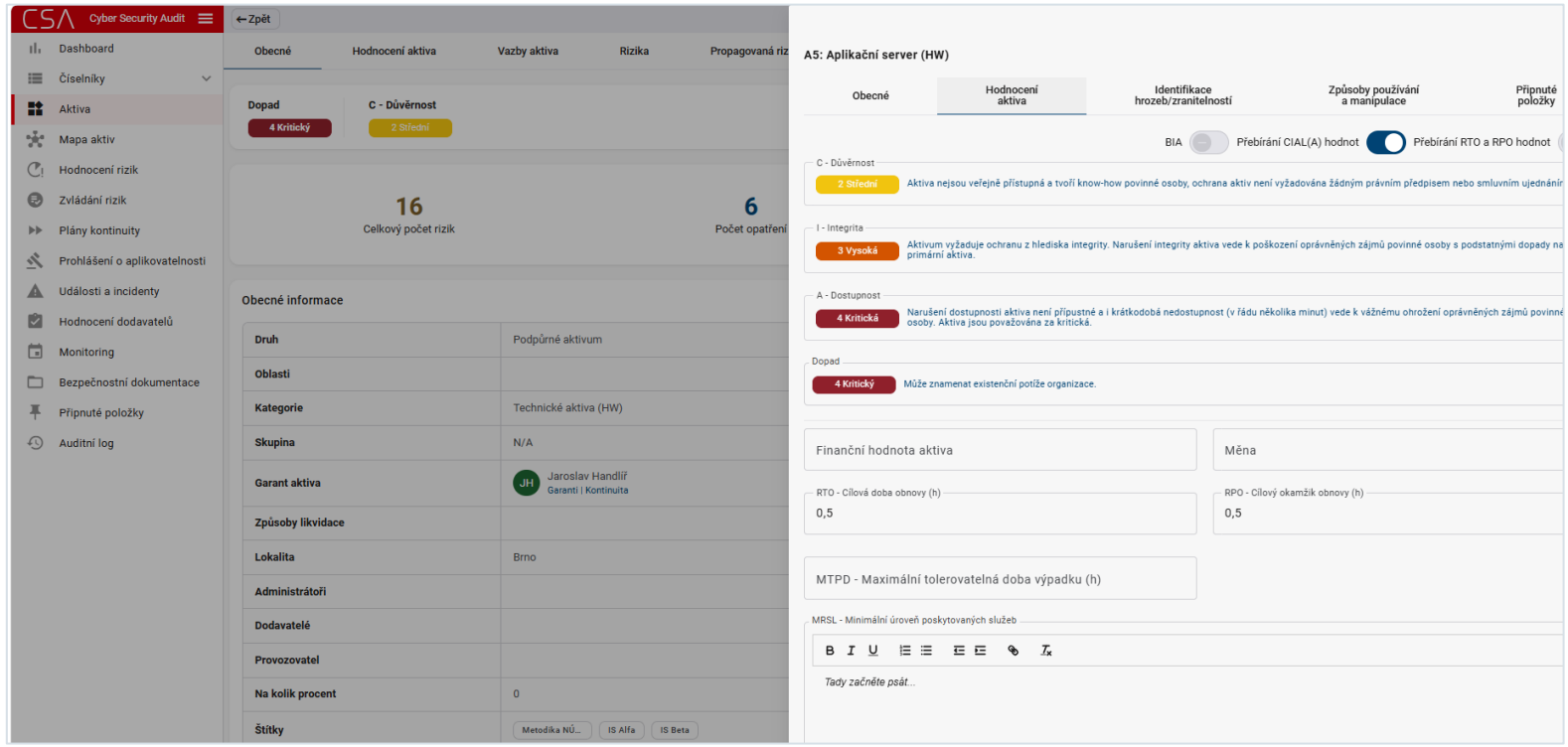
Mapa aktiv



Závislosti jsou klíčové

- Primární a podpůrná aktiva
- Dopad selhání napříč vazbami

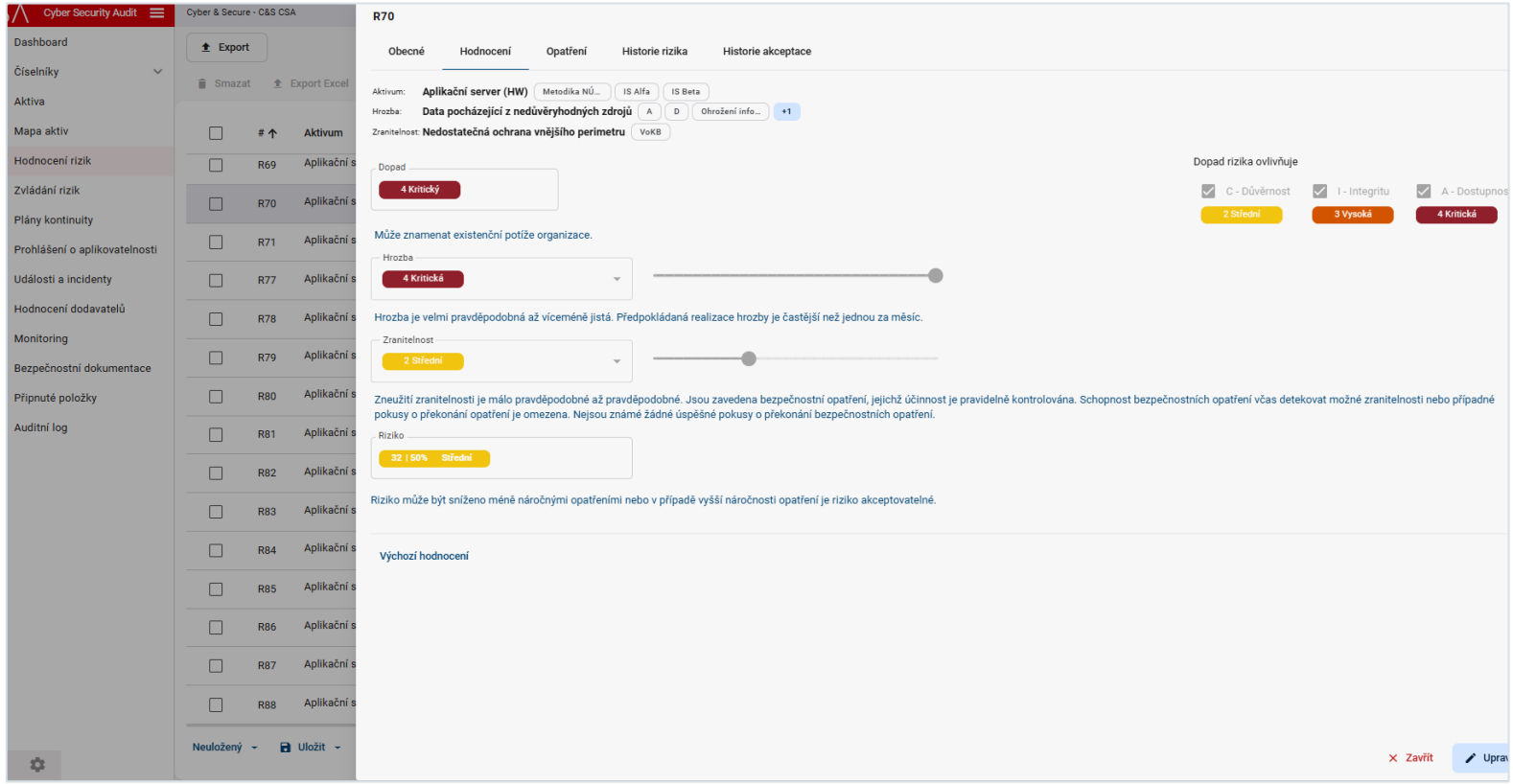
Hodnocení aktiv



Od aktiva k hrozbě

- Hodnocení aktiv
- Relevantní hrozby a zranitelnosti

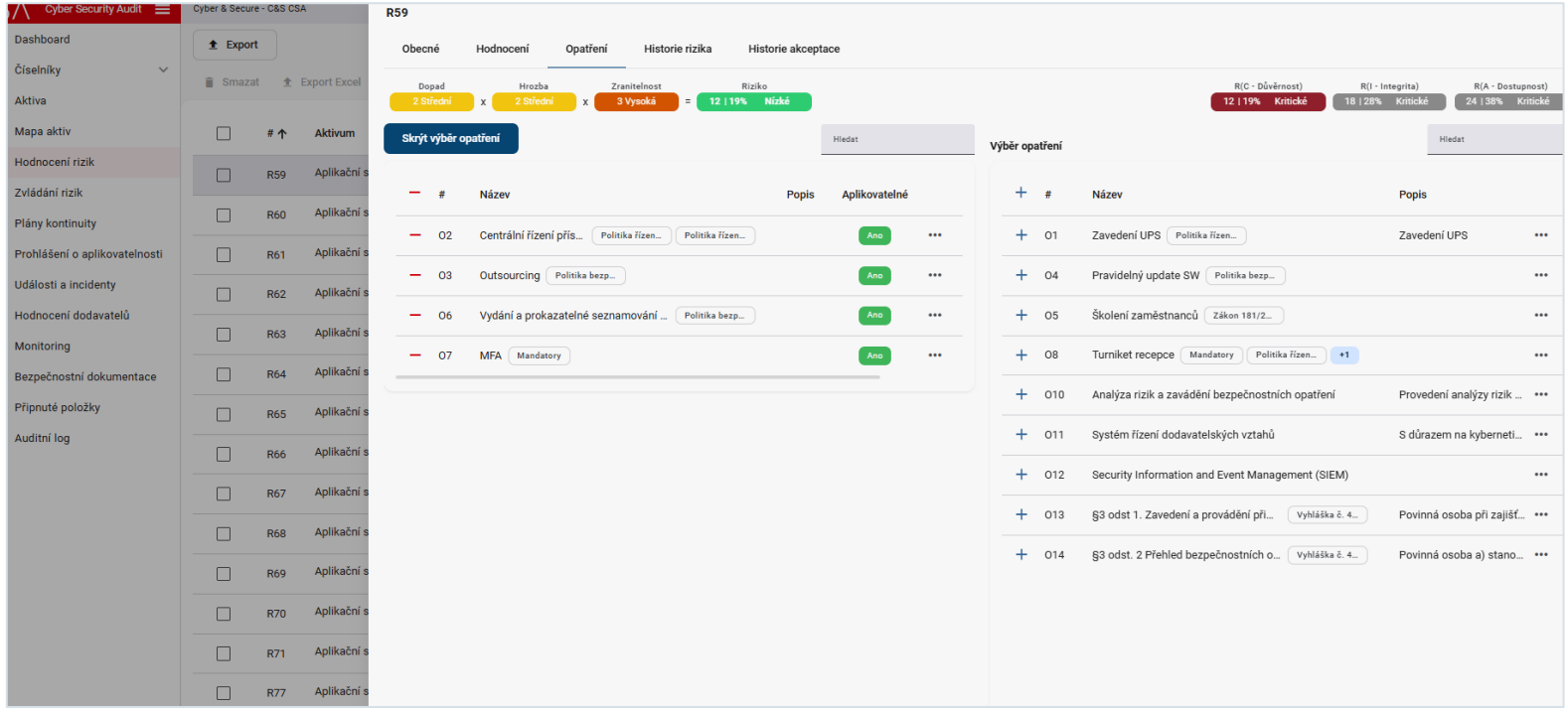
Hodnocení rizik



Která rizika řešit nejdřív?

- Hromadné hodnocení
- Filtry a vlastní pohledy

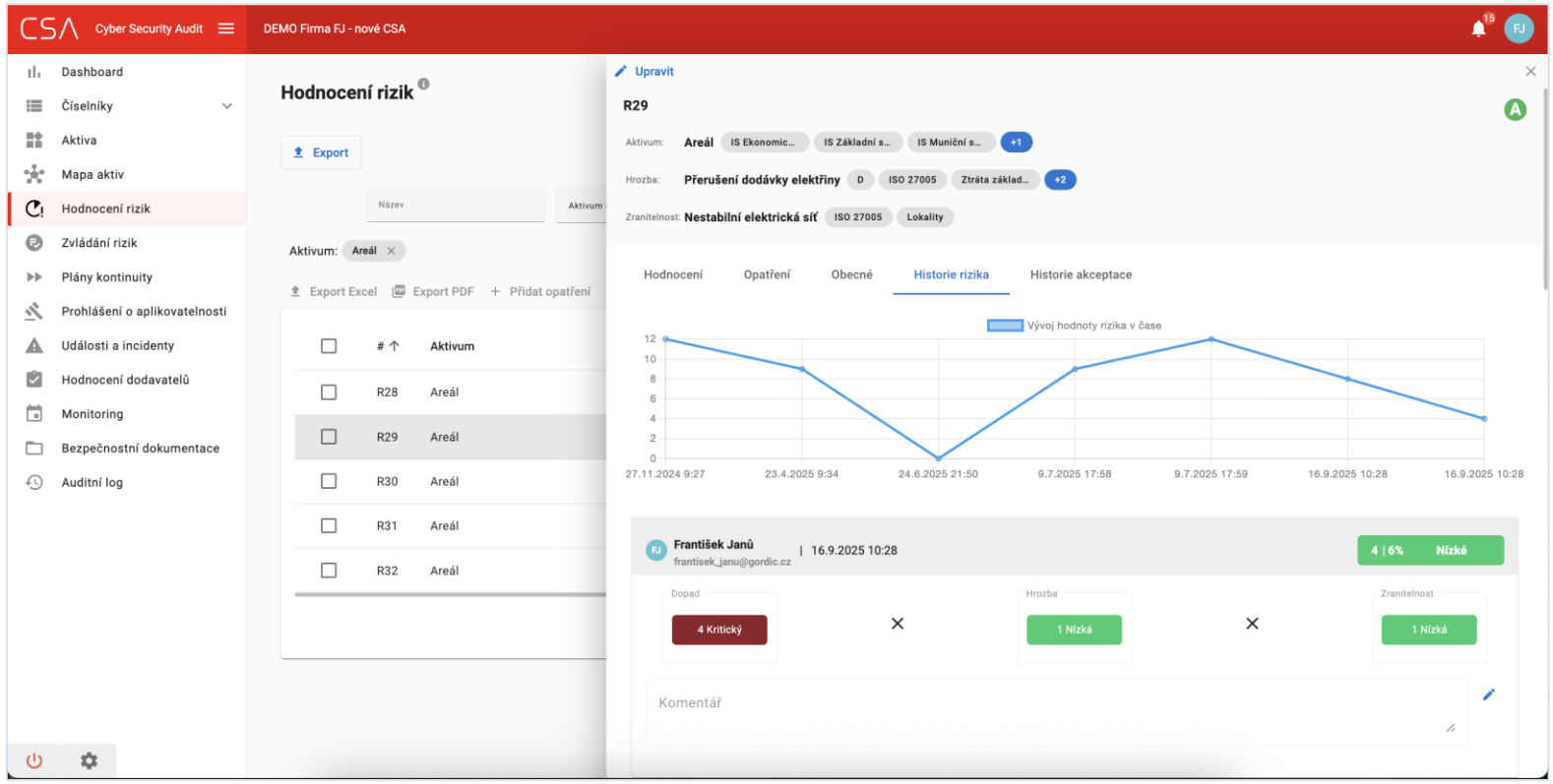
Zavedení opatření a snížení rizika



Opatření mění výsledek

- Výchozí hodnocení lze upravit
- Po zavedení opatření sledujeme snížení rizika

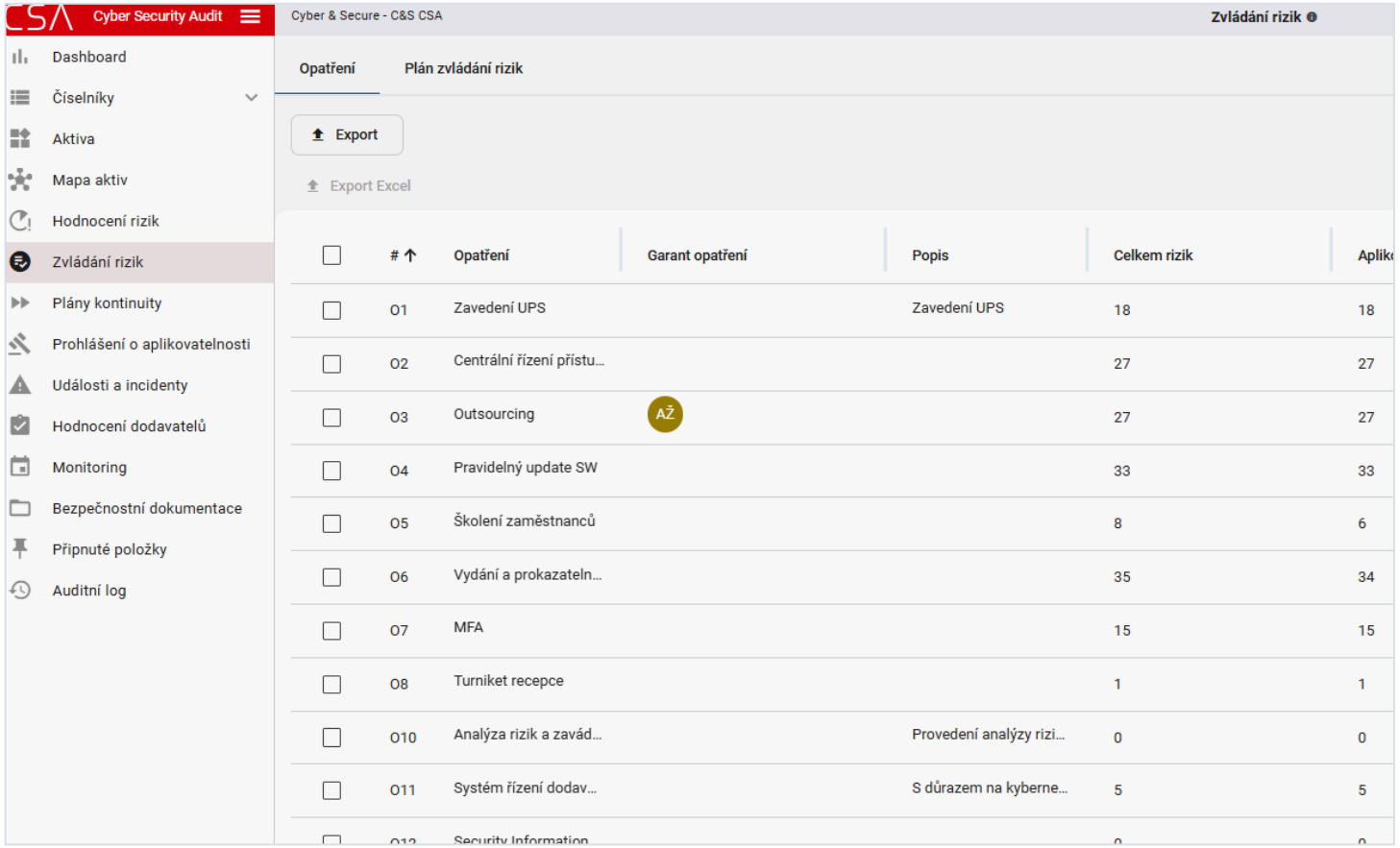
Detail rizika a jeho vývoj



Riziko má svůj vývoj

- Detail před a po opatření
- Akceptace a monitoring

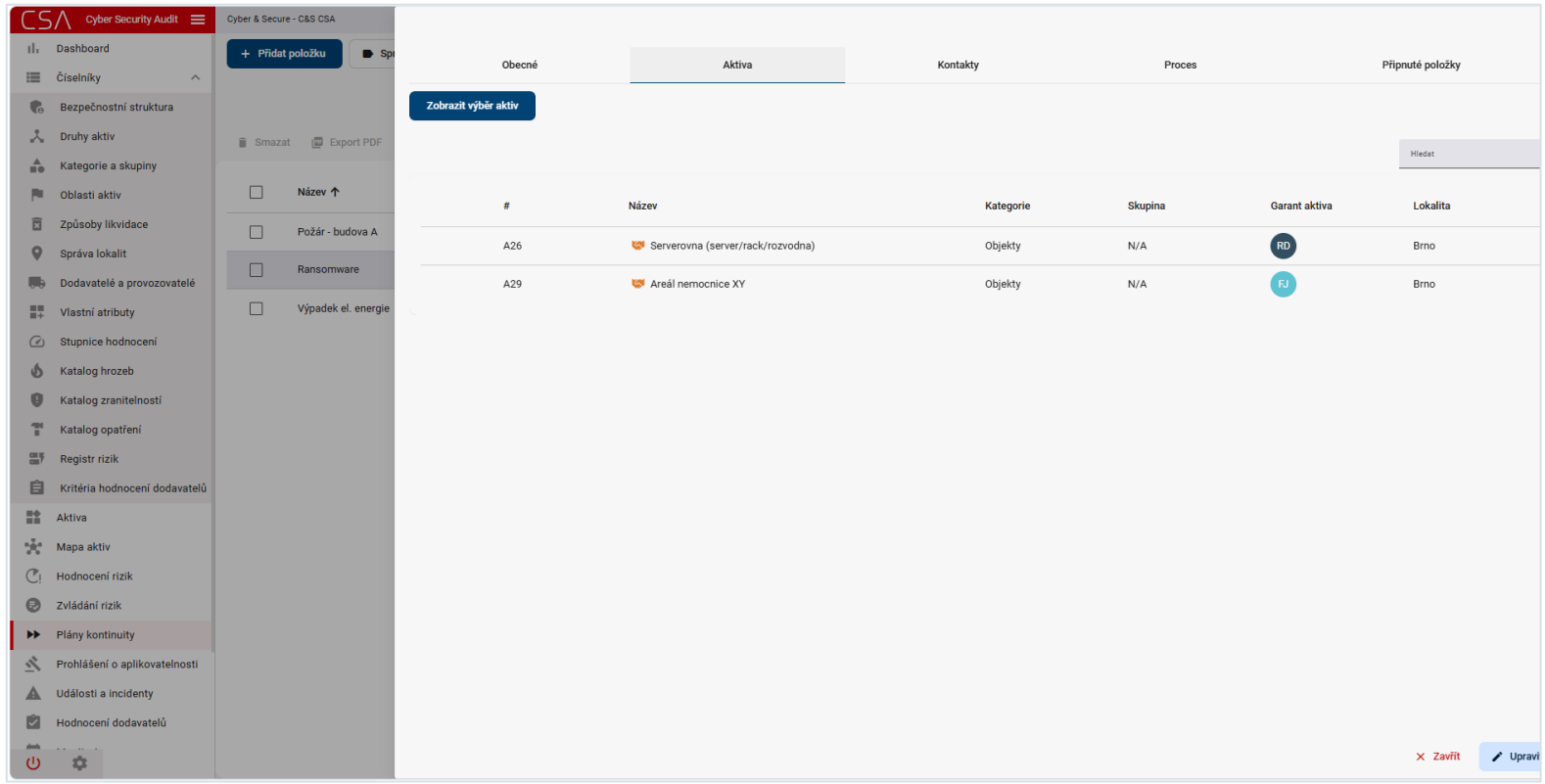
Plán zvládání rizik



Z hodnocení vzniká plán

- Konkrétní opatření a jejich stav
- Potřebné finance a kapacity

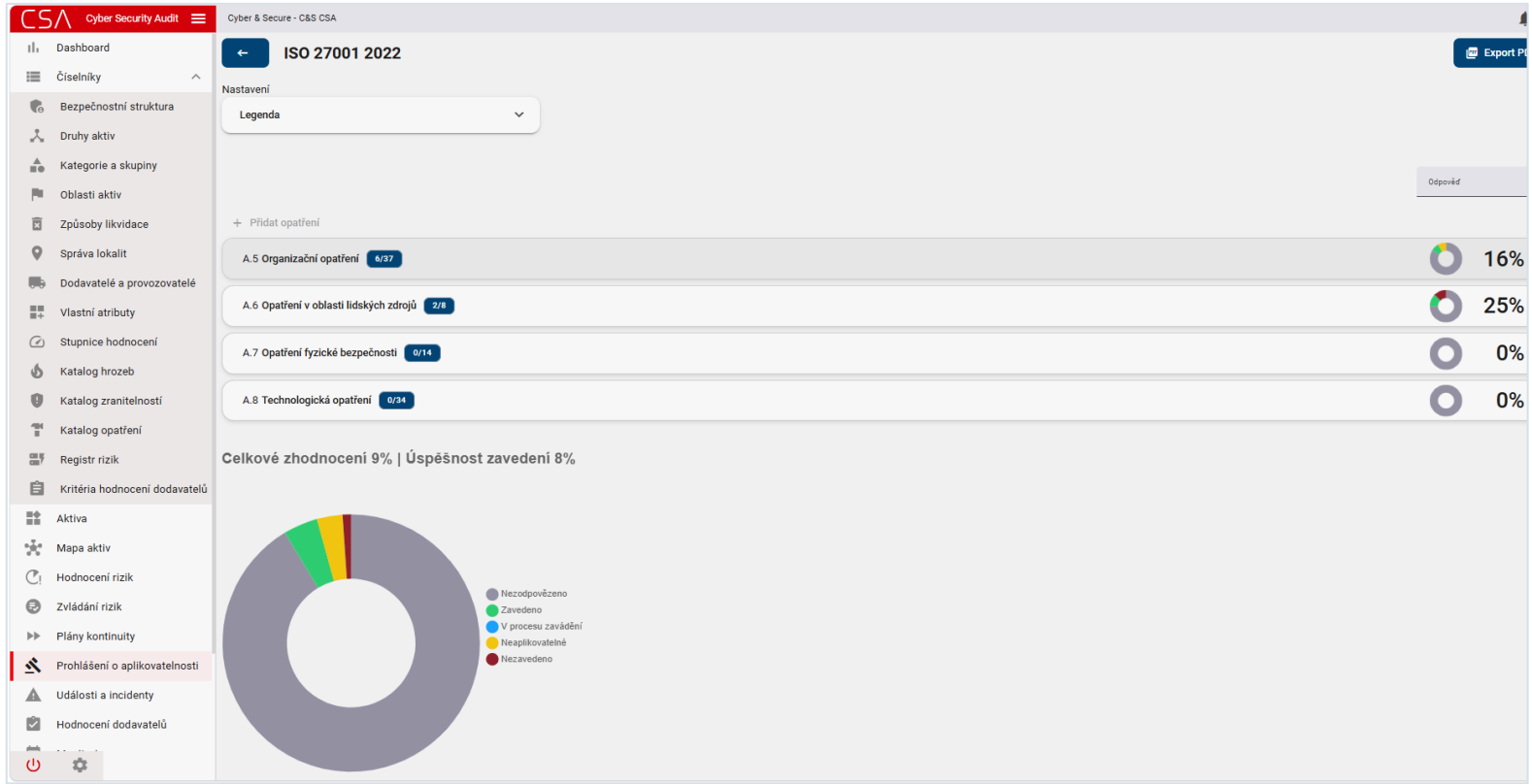
Plány kontinuity



Když dojde k výpadku

- Popis návazného postupu
- Kontakty a dotčená aktiva

Prohlášení o aplikovatelnosti

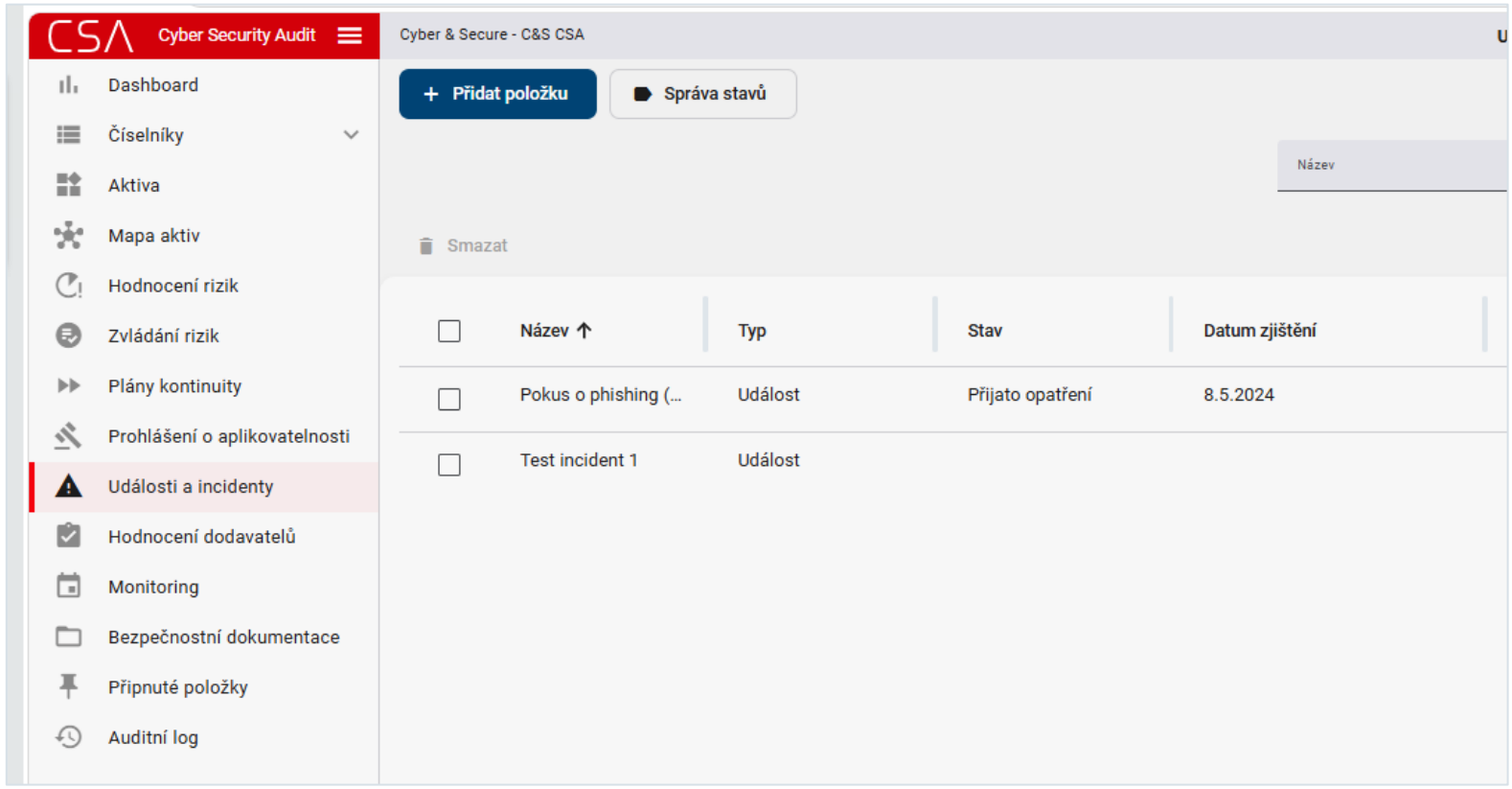


Jedna evidence, více využití

- self audit, GAP analýza
- ZoKB, ISO 27000, DORA …

GORDIC

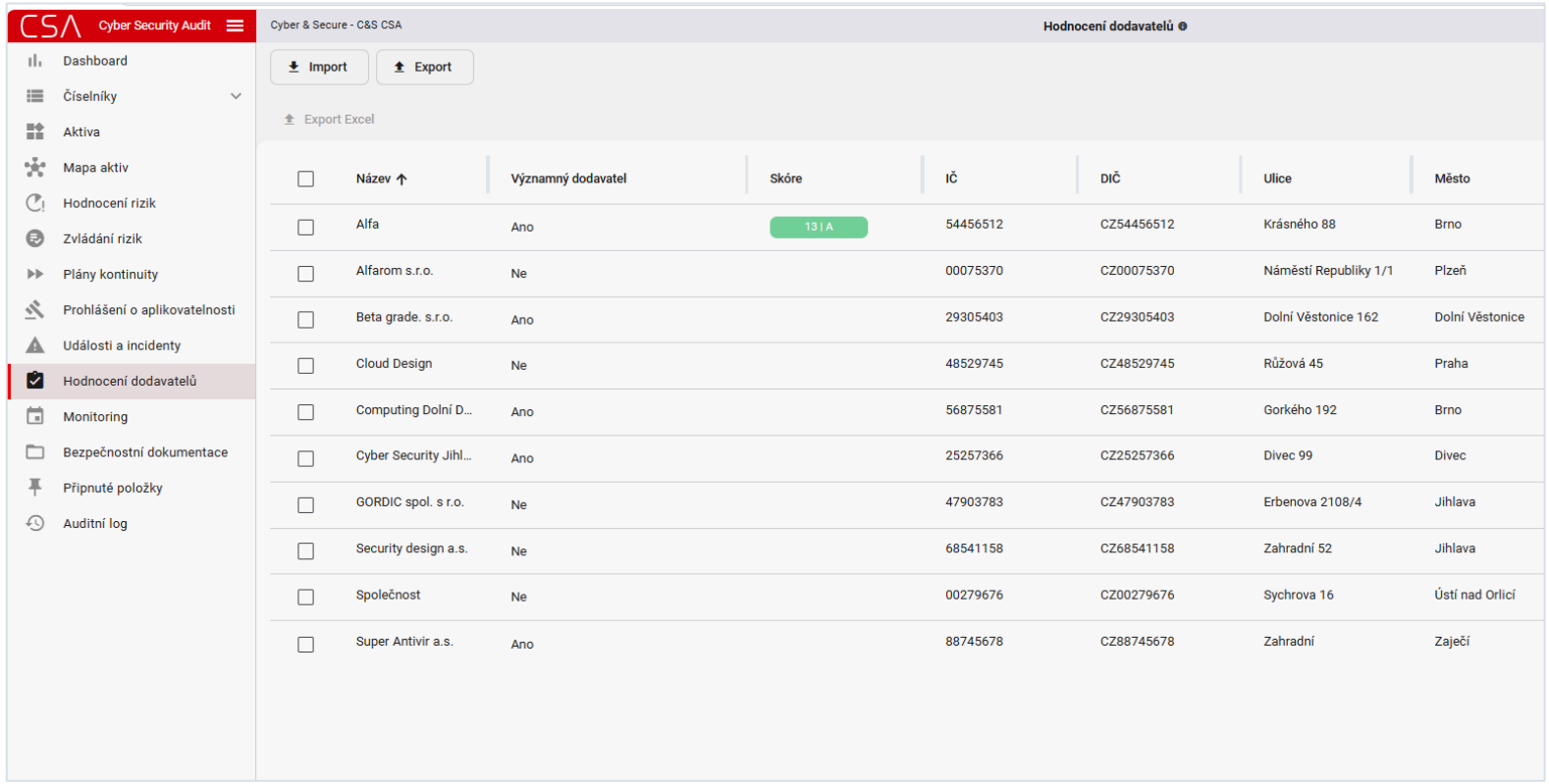
Bezpečnostní události a incidenty



Rizika nekončí analýzou

- Evidence událostí a incidentů
- Detail a dohledatelnost

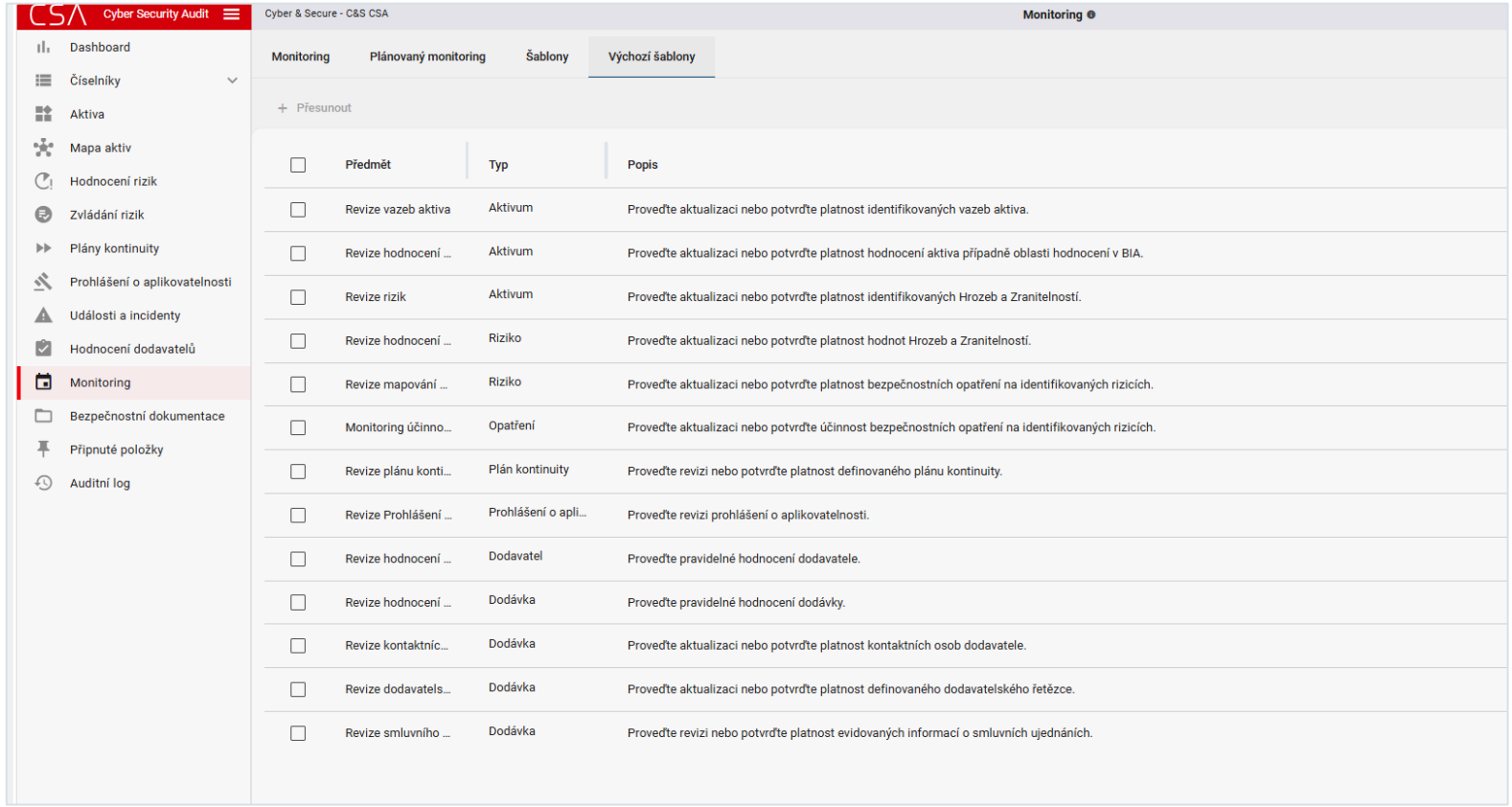
Hodnocení dodavatelů



Dodavatel je součást rizika

- Evidence významných dodavatelů
- Hodnocení podle vlastních kritérií

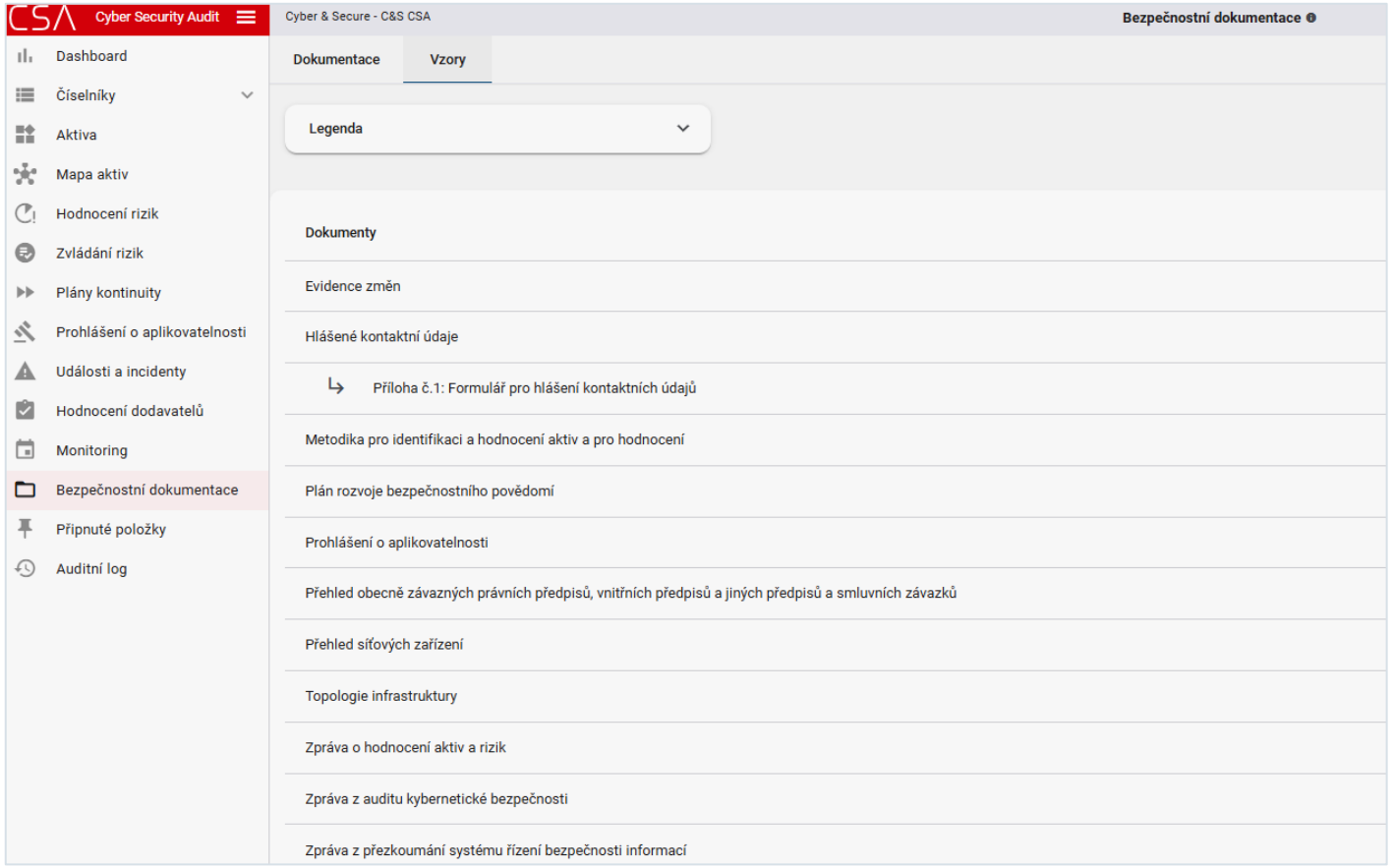
Monitoring



Průběžné sledování

- Úkoly a termíny
- E-mailové upomínky

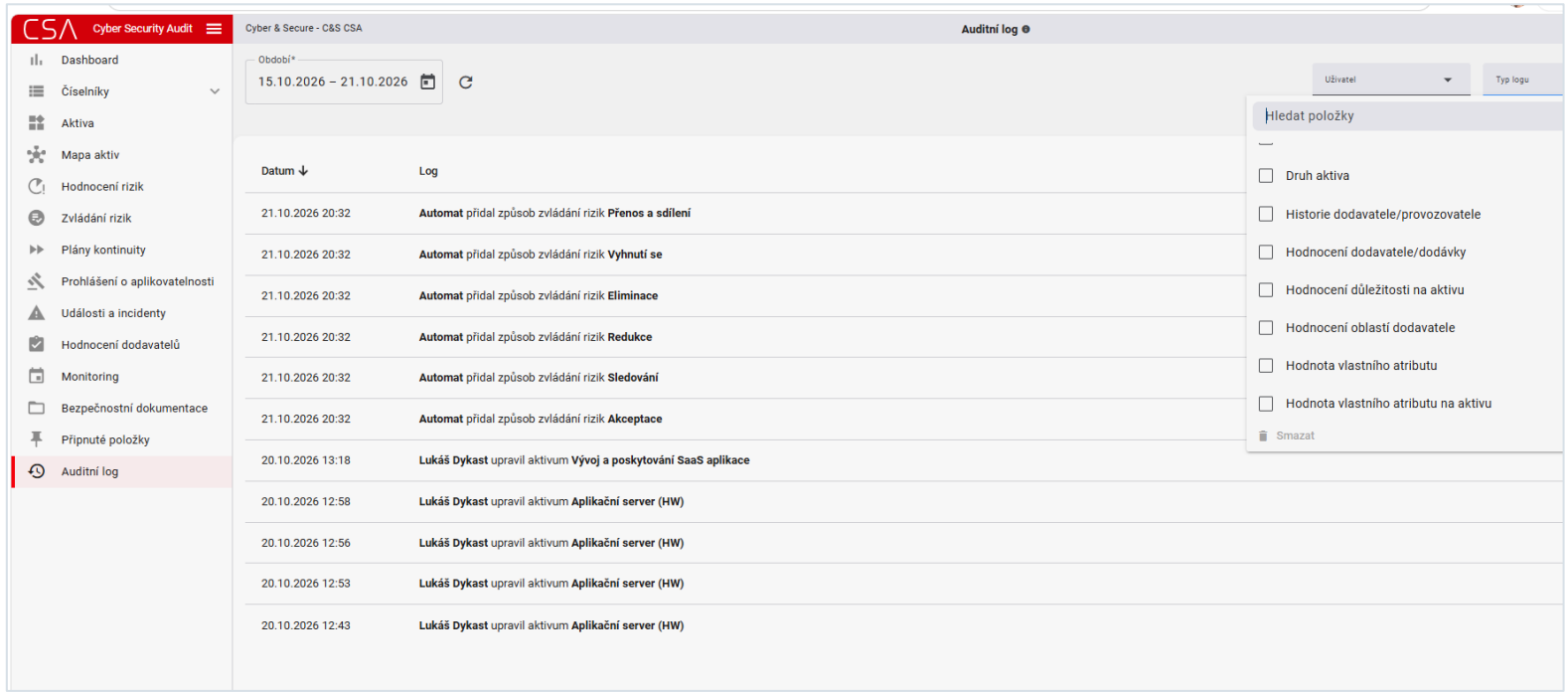
Bezpečnostní dokumentace



Podklady na jednom místě

- Vzory bezpečnostní dokumentace
- Podpora návazných procesů

Auditní log



Prokazatelnost a integrace

- Auditní stopa provedených operací
- REST API / syslog pro SIEM

Řešení GORDIC pro kyberbezpečnost

Školení a konzultace

Webináře a záznamy
Individuální školení a e-learning
www.gordic.cz/skoleni

CSA

Analýza a řízení kybernetických rizik

GORDIC

GDPO

E-learning, Moodle / SCORM
Phishingové kampaně a kurzy KB

GDA

GDPR a metodika ÚOOÚ

Reference




TSMO


ÚŘAD PRO CIVILNÍ LETECTVÍ


EOP
ELEKTRÁRNY
OPATOVICE


TEPLÁRNY
BRNO


Benešov


UNITED
ENERGY
Váš zdroj tepelné pohody


jihočeské
nemocnice


Draslovka


PROGRESSIVE
PSTCLC
LOGISTICS
MITSUI-SOKO GROUP


energy
Energie pro budoucnost a stabilitu


innogy



Děkuji za pozornost

Eliška Bartůšková, MBA
eliska_bartuskova@gordic.cz
+420 725 056 390
www.gordic.cz