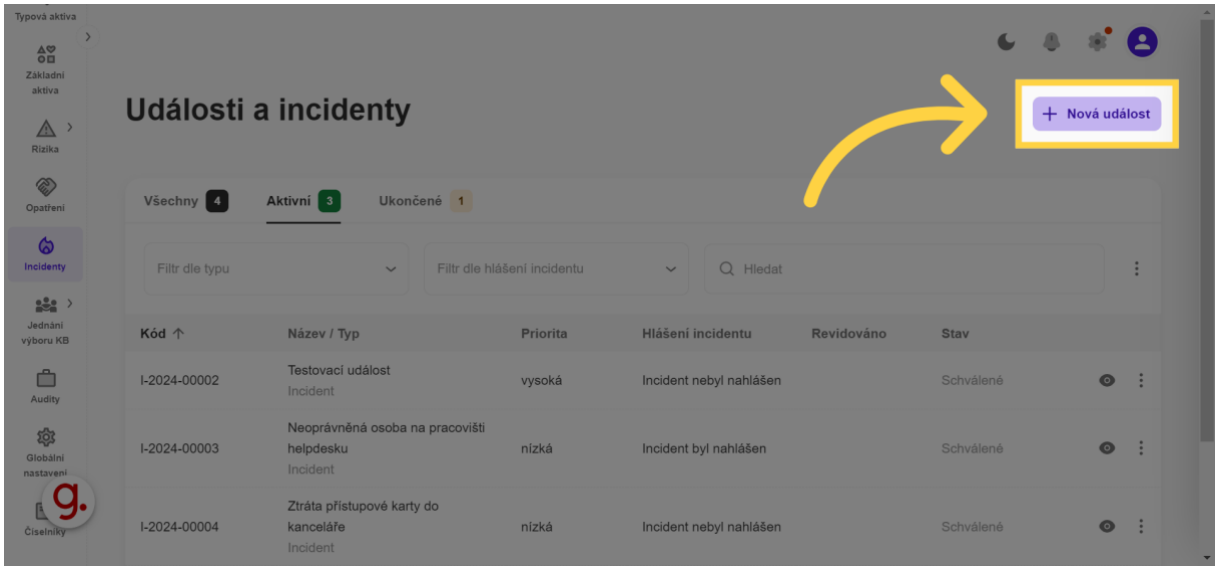
Události a incidenty

Kybernetický bezpečnostní incident je narušení bezpečnosti aktiv v důsledku kybernetické bezpečnostní události. Jedná se o situaci, kdy byla porušena kybernetická bezpečnost. V tomto videu vám ukážeme, jak zaevidovat událost a jak ji zpracovat, pokud je následně vyhodnocena jako incident.

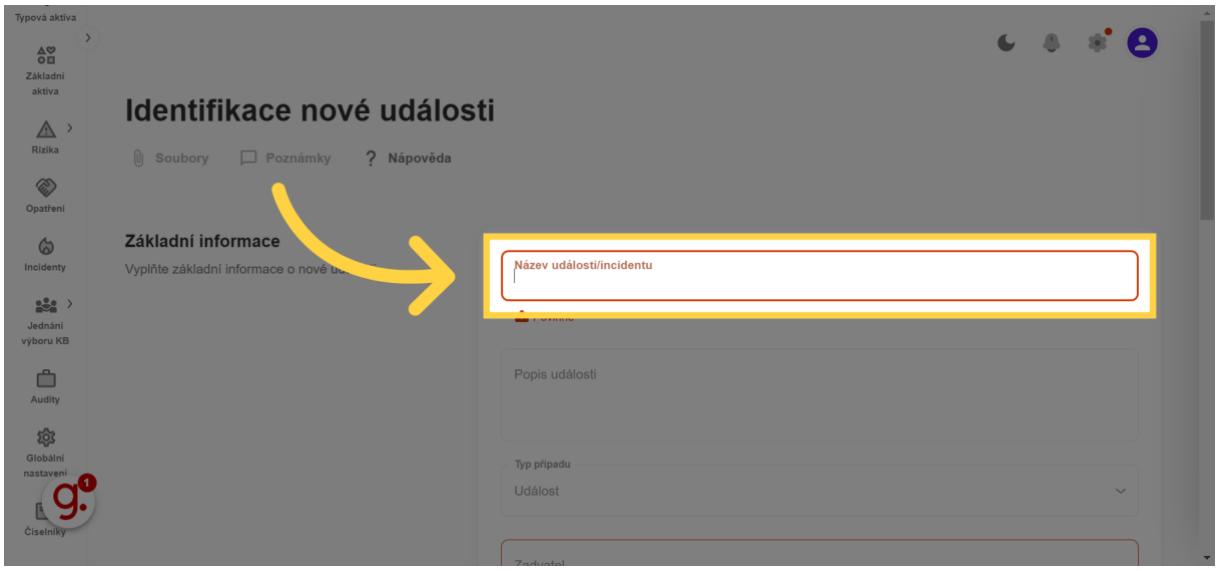
1. Nová událost

Pro zaevidování nové události klikněte na tlačítko "Nová událost".



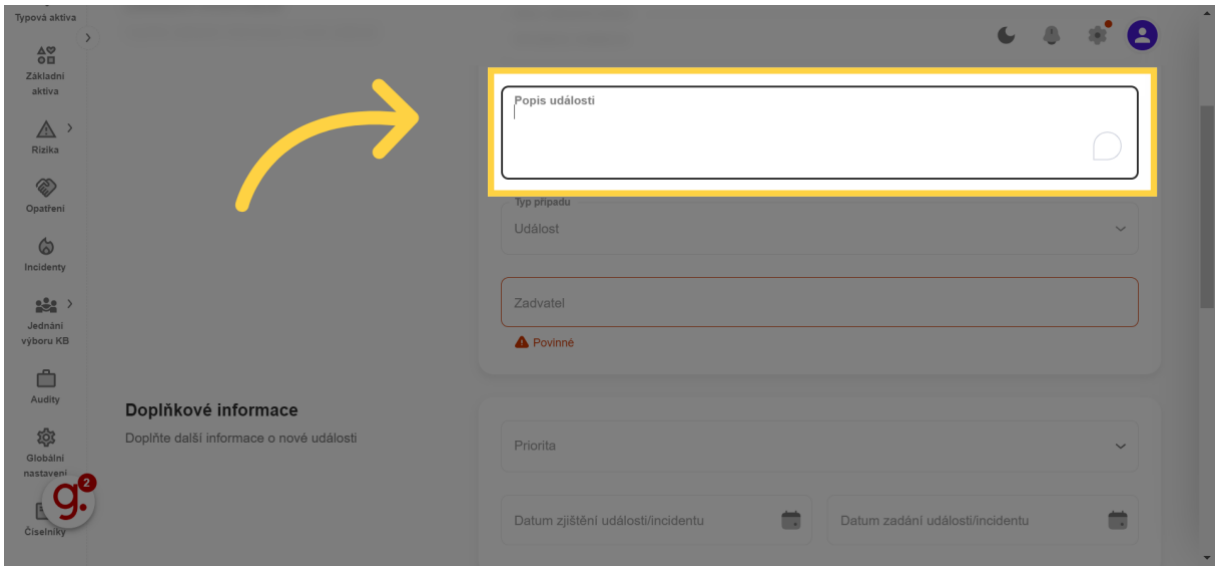
2. Název

Zadejte jednoznačné a jasné pojmenování nové události.



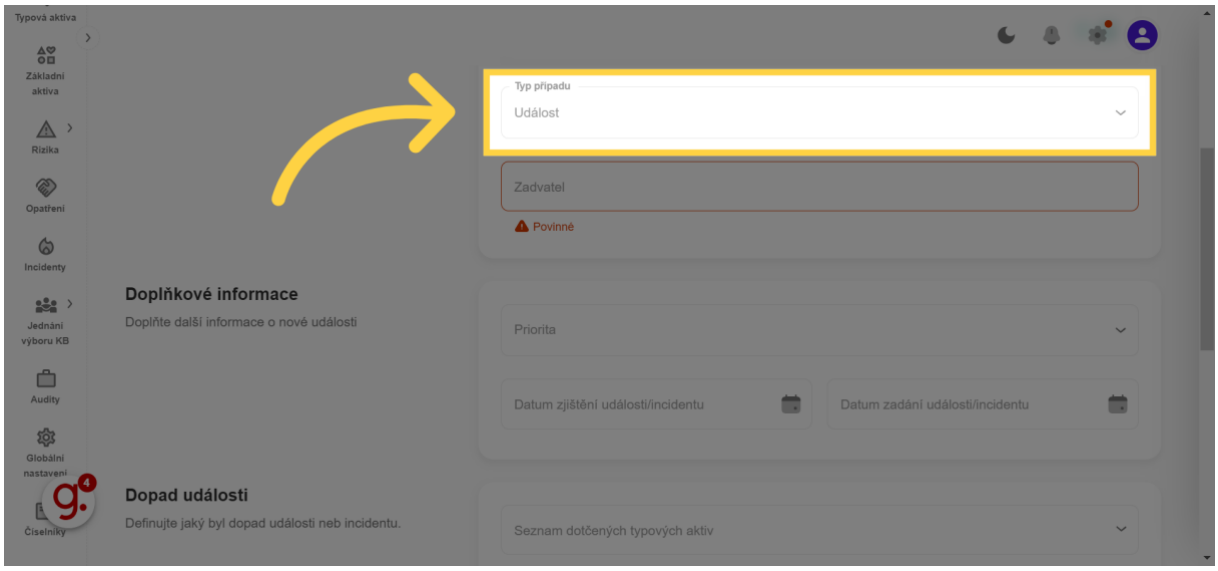
3. Popis

Vyplňte dostatečně podrobný slovní popis, který doplňuje název záznamu o informace důležité pro správné pochopení, co záznam reprezentuje.



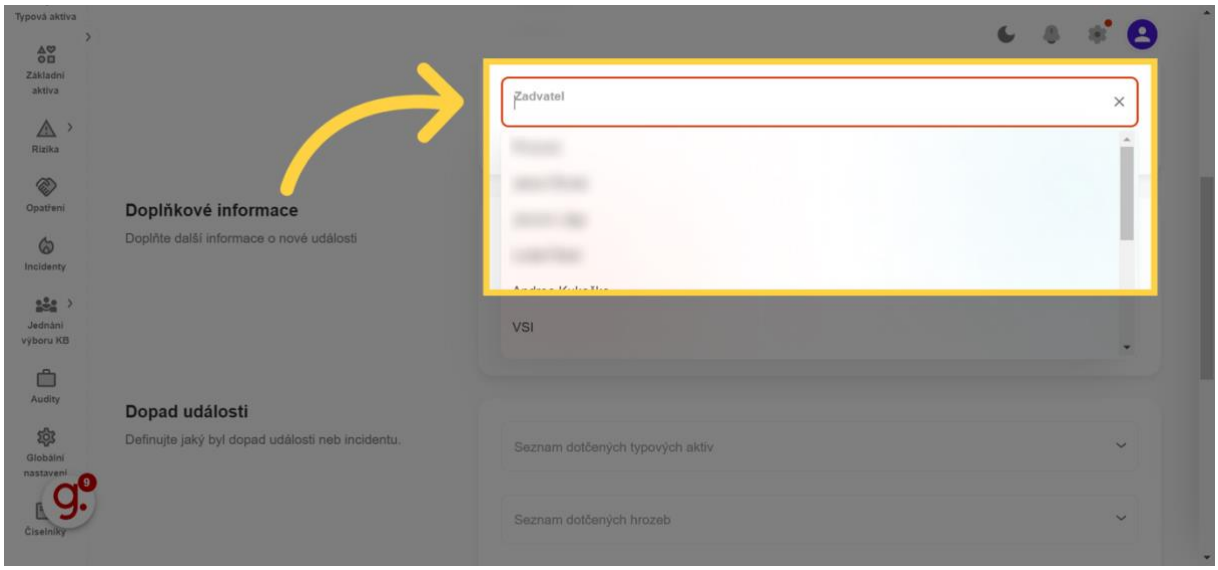
4. Událost

Při zadávání je případ automaticky klasifikován jako událost.



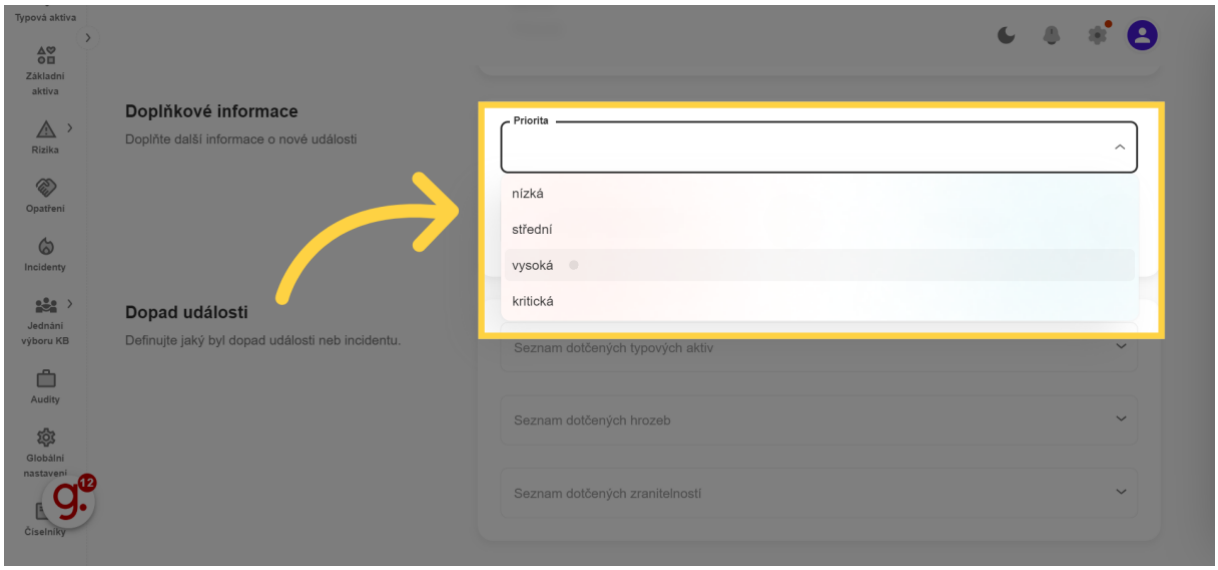
5. Zadavatel

Zadavatelem je osoba, která vytvořila a zaznamenala událost. MoyaKybeon nabízí osoby, které již byly dříve v rámci systému využity. Můžete vybrat z nabídky, nebo doplnit někoho nového.



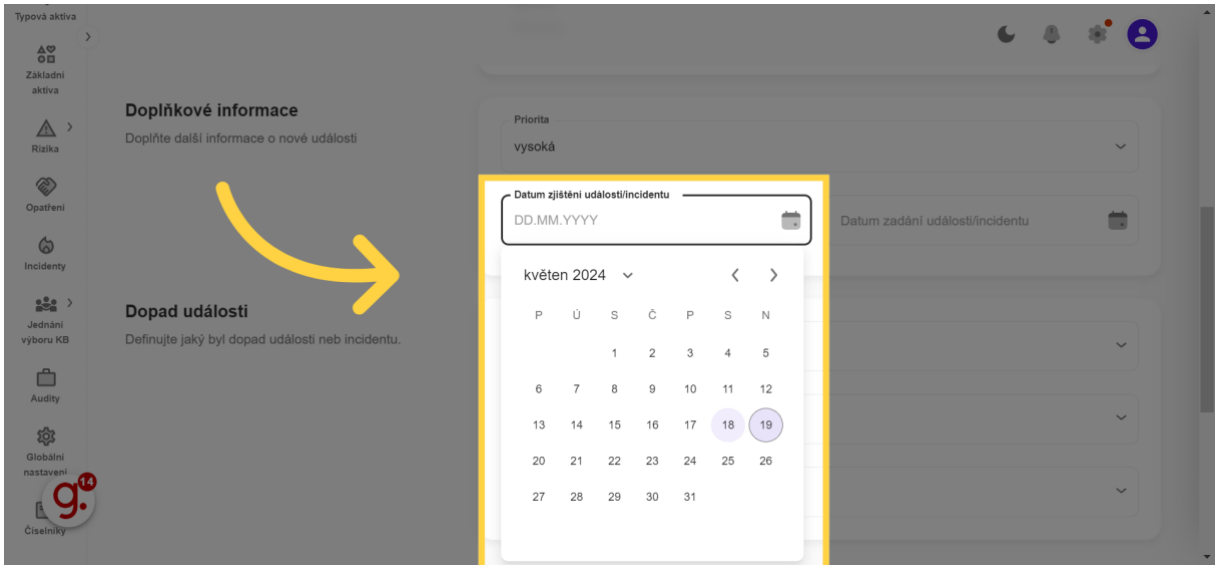
6. Priorita

Zadejte prioritu události.



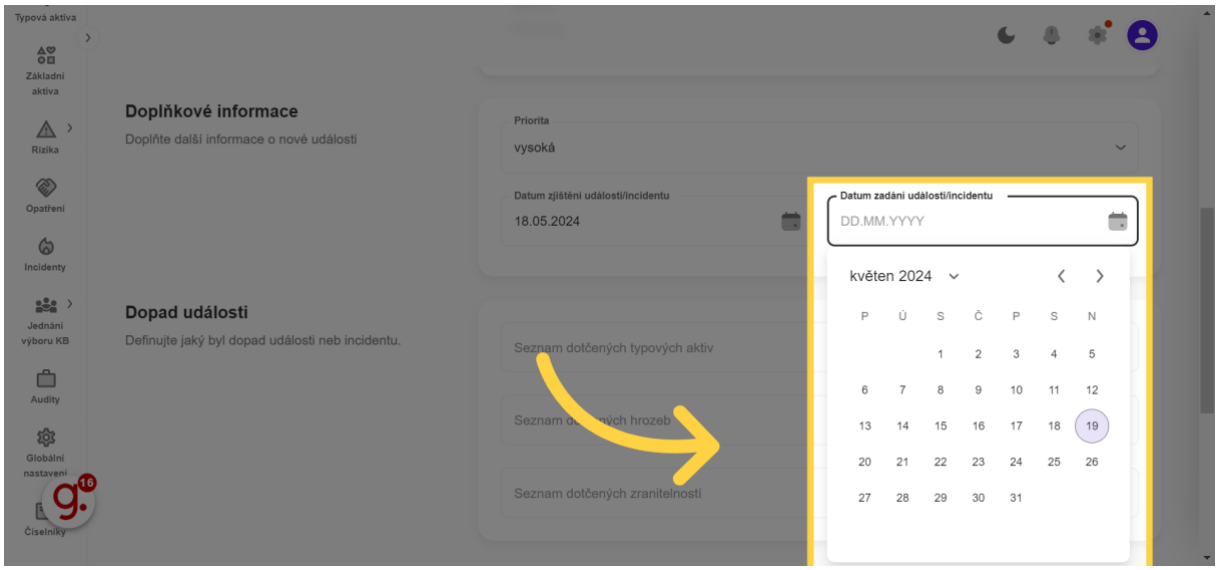
7. Datum zjištění události

Zaznamenejte datum zjištění události.



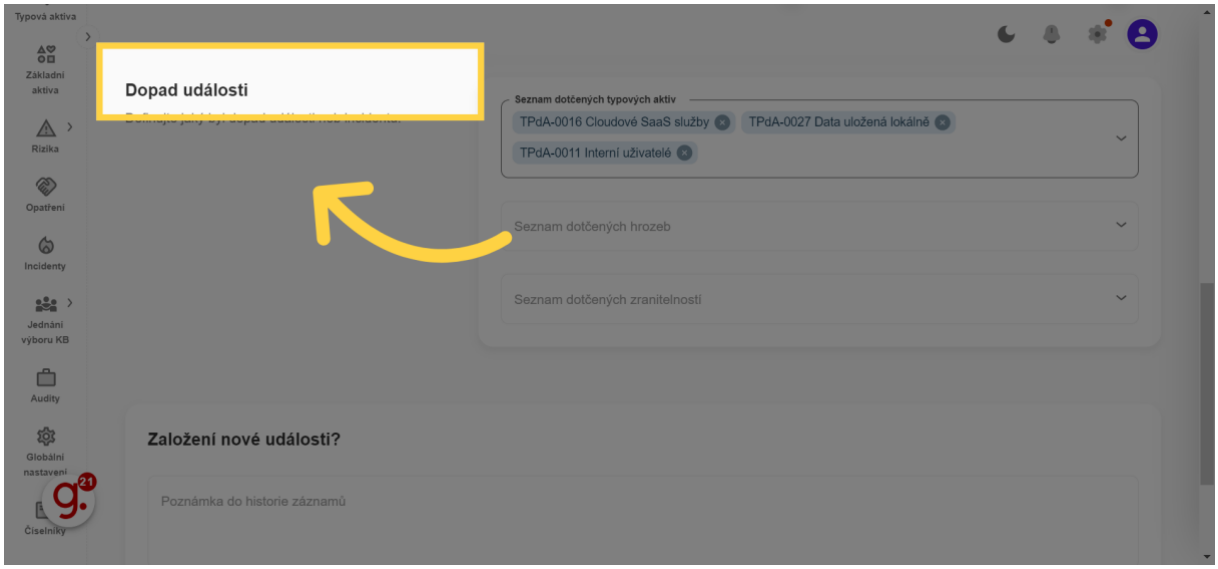
8. Datum zadání do MoyaKybeon

A také datum zadání do systému MoyaKybeon.



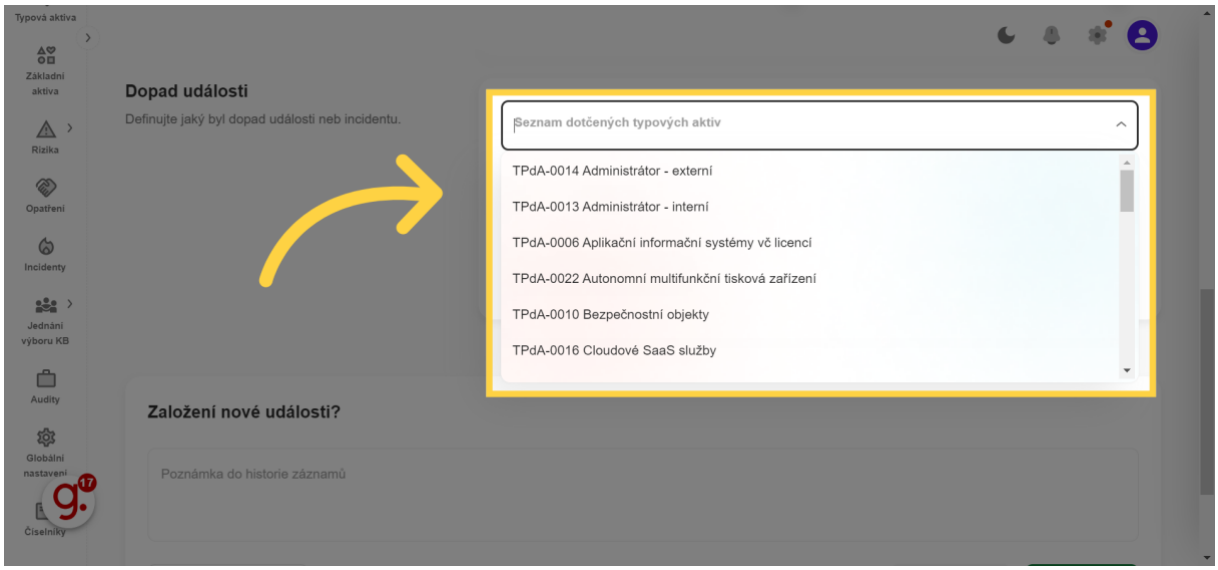
9. Dopad

Po vyplnění základních údajů je potřeba zmapovat rozsah a dopad události.



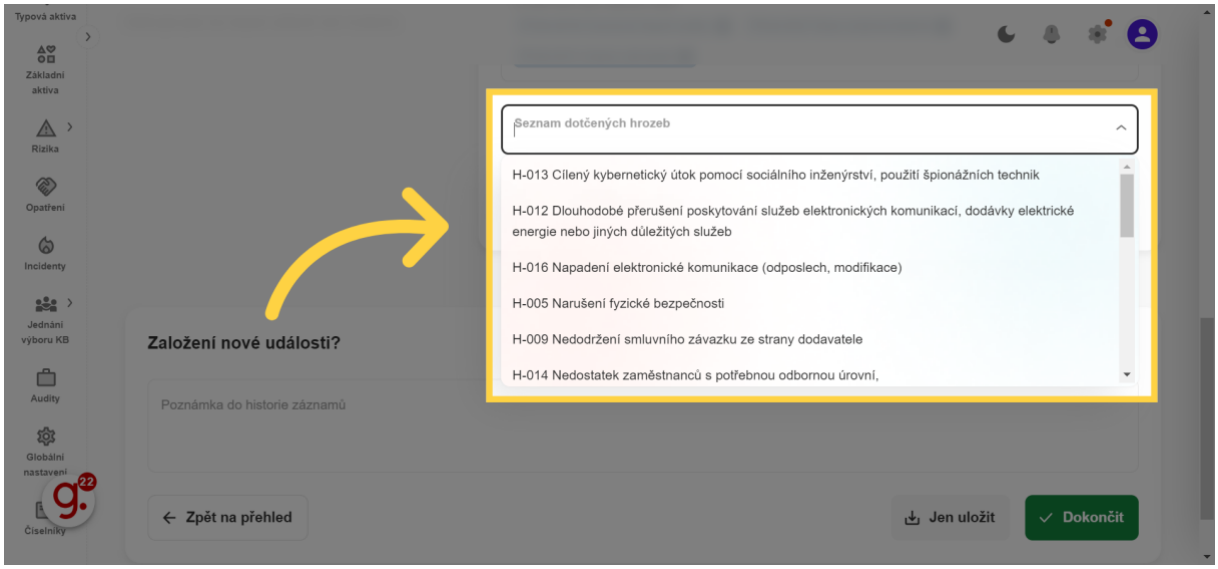
10. Typová aktiva

Zvolte všechna typová podpůrná aktiva, která byla bezpečnostní událostí dotčena.



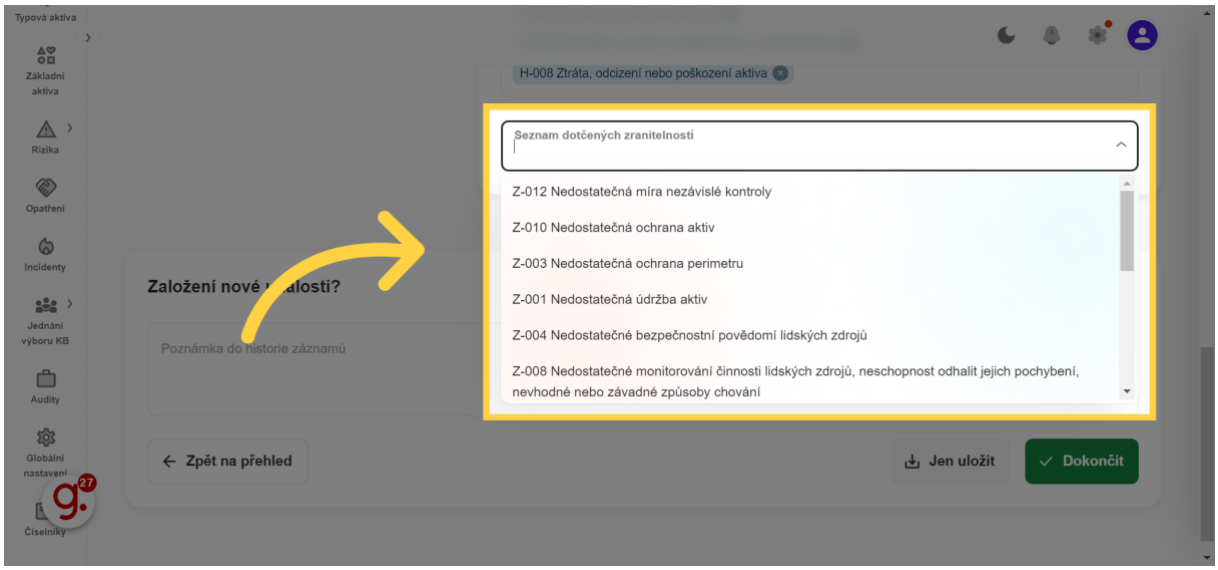
11. Hrozby

Vyberte všechny hrozby, které při bezpečnostní události působily.



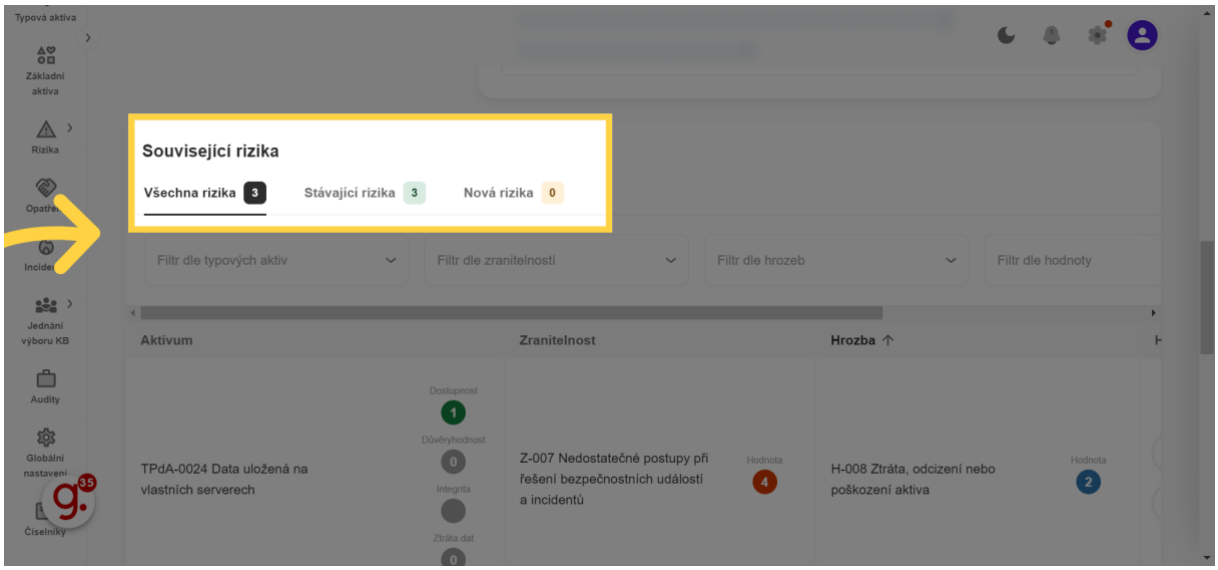
12. Zranitelnosti

A také vyberte všechny zranitelnosti, které bezpečnostní událost umožnily.



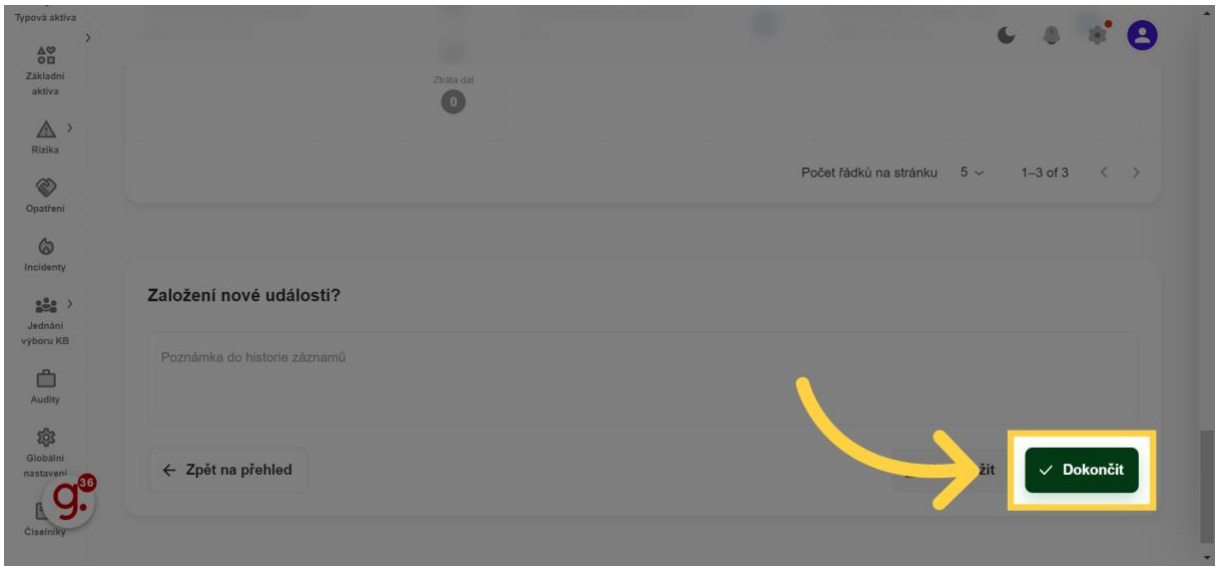
13. Rizika

Po nadefinování dopadu MoyaKybeon automaticky zobrazí všechna související rizika z katalogu rizik.



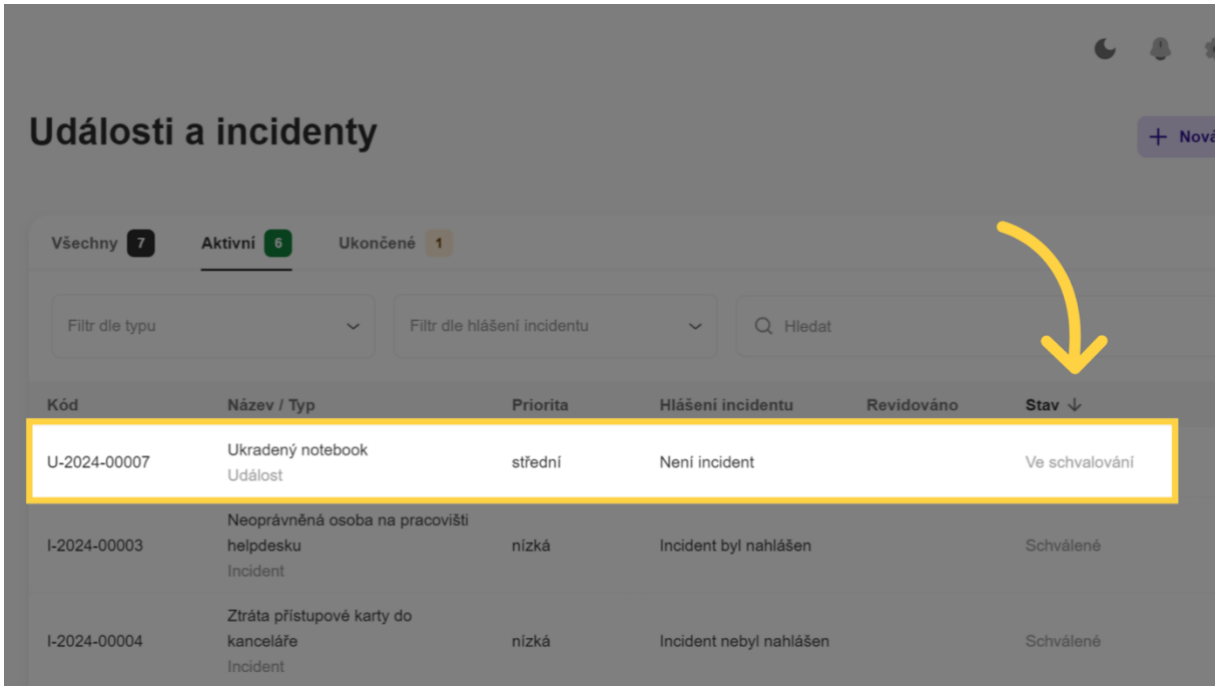
14. Dokončit 1

Kliknutím na "Dokončit" zaevidujete novou bezpečnostní událost. Tu je nutno dále vyhodnotit a rozhodnout, zda se jedná o incident (a je tedy potřeba učinit dodatečné kroky).



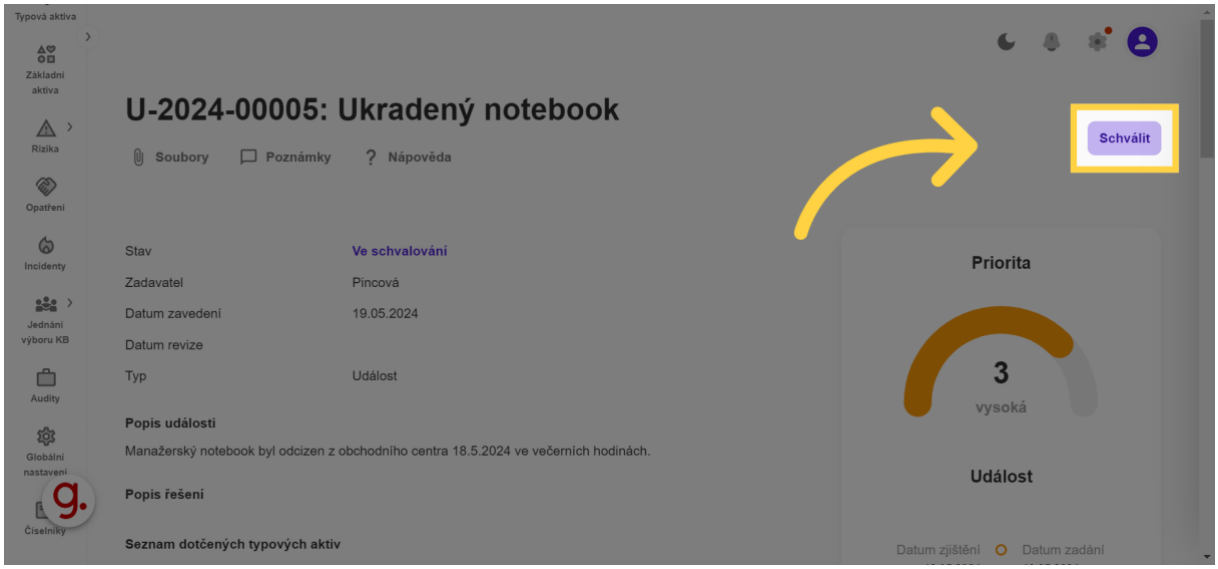
15. Přehled

Každou novou událost je potřeba schválit a vyhodnotit.



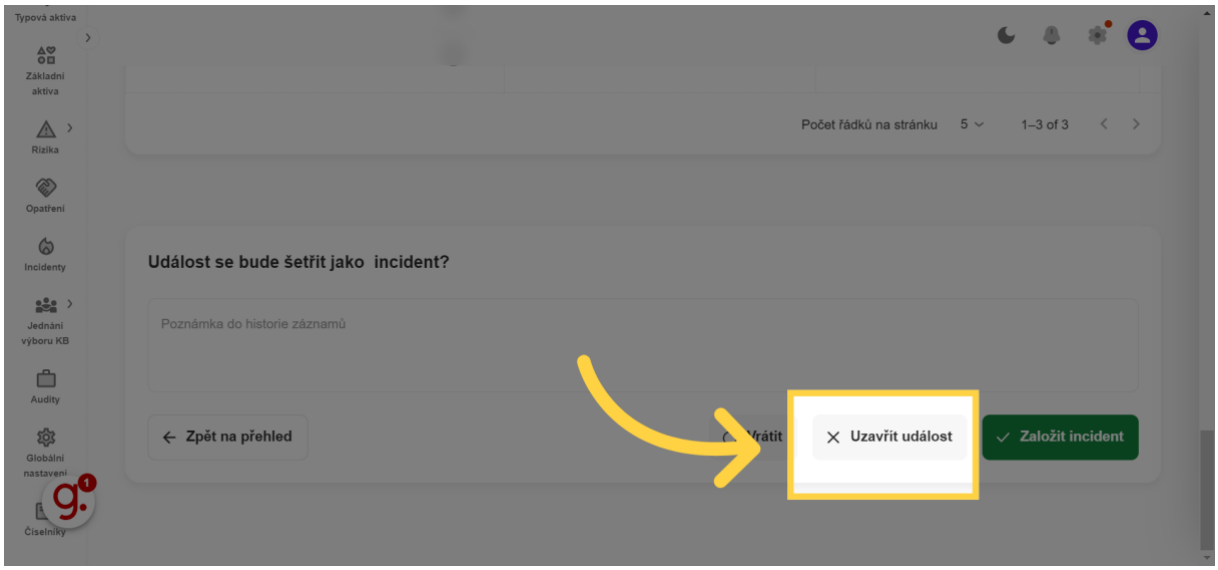
16. Schválení

Stejně jako kdekoli jinde v aplikaci, i u událostí máte tlačítka k akci v záhlaví každé detailní karty.



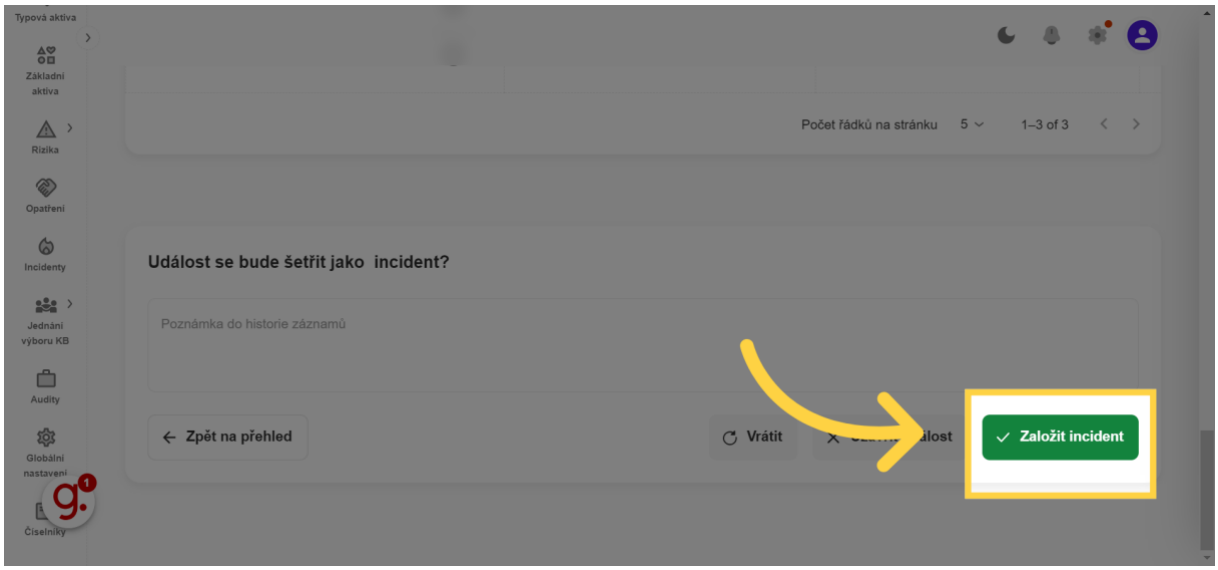
17. Uzavření

Schvalovatel rozhoduje, zda se jedná pouze o událost. Pokud ano, tlačítkem "Uzavřít událost" ji uzavře a v MoyaKybeon již nebude nutné podnikat další kroky.



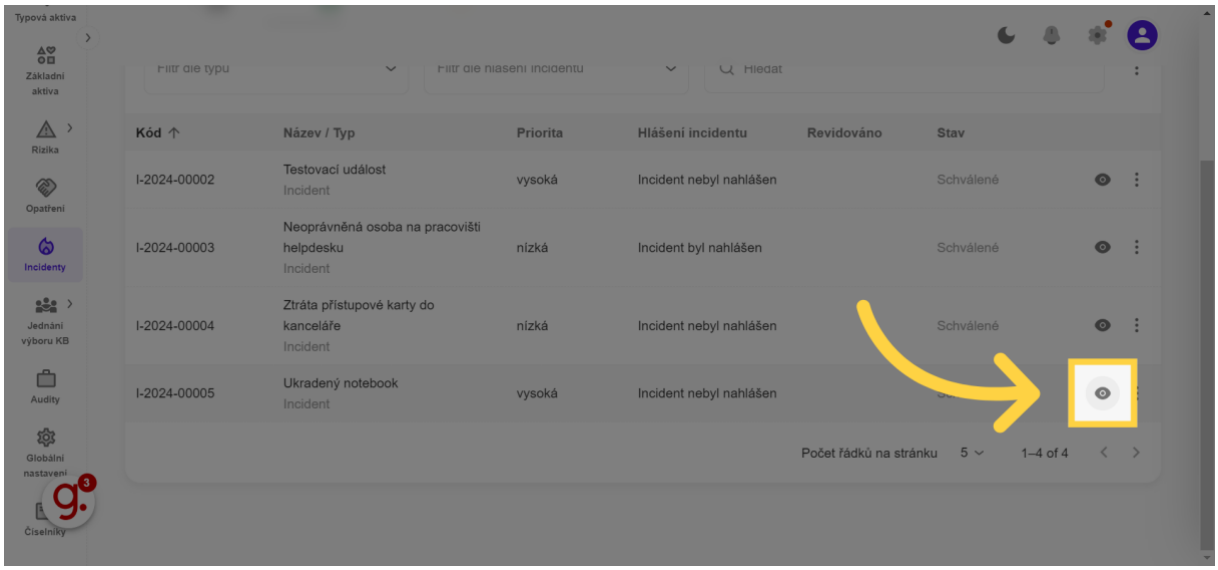
18. Založení incidentu

V případě, že se jedná o incident, tlačítkem "Založit incident" se spustí následné administrativní kroky v MoyaKybeon.



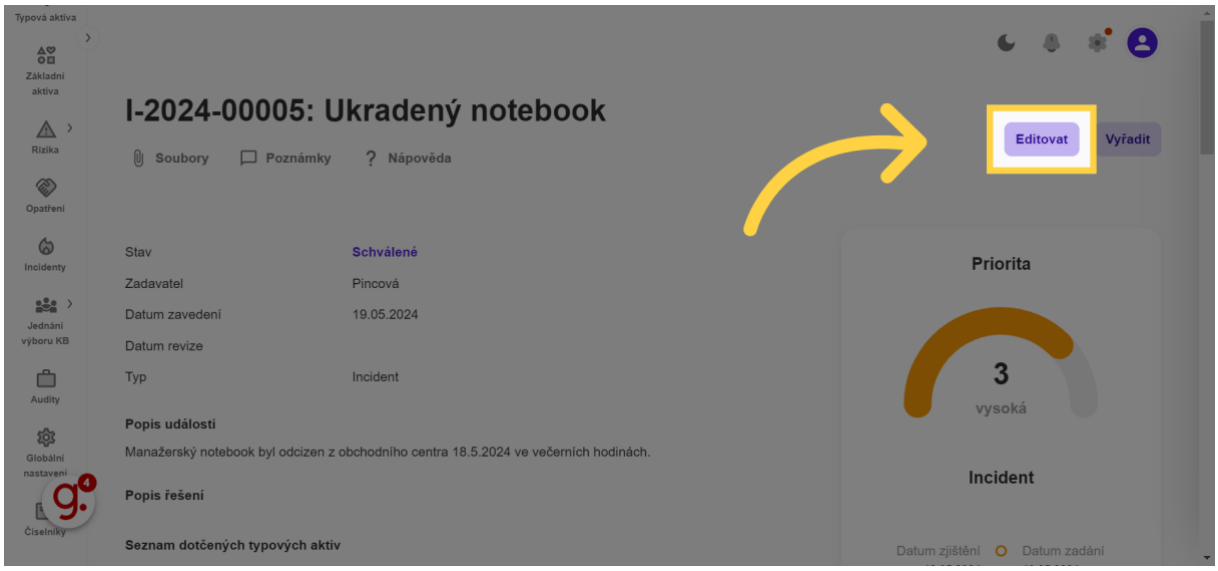
19. Detail

Pojďme se dále podívat, co je potřeba zaznamenat, pokud schvalovatel řekl, že je potřeba událost překlasifikovat na incident. Detaily incidentu si otevřete z přehledu.



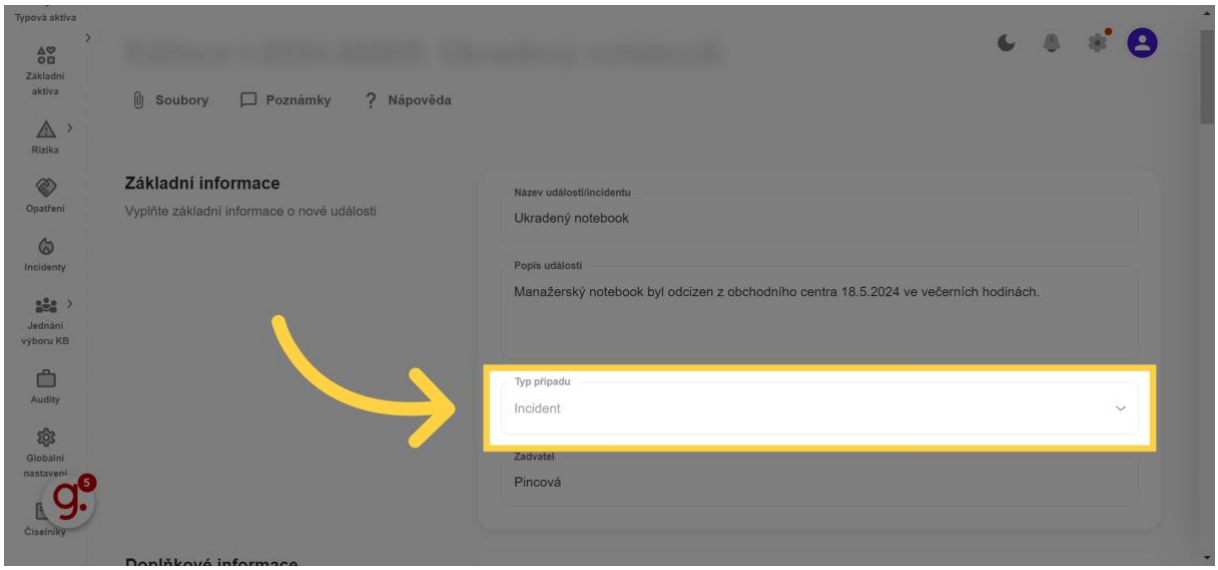
20. Editace

Tlačítko "Editovat" umožní doplnit do evidence další provedené kroky.



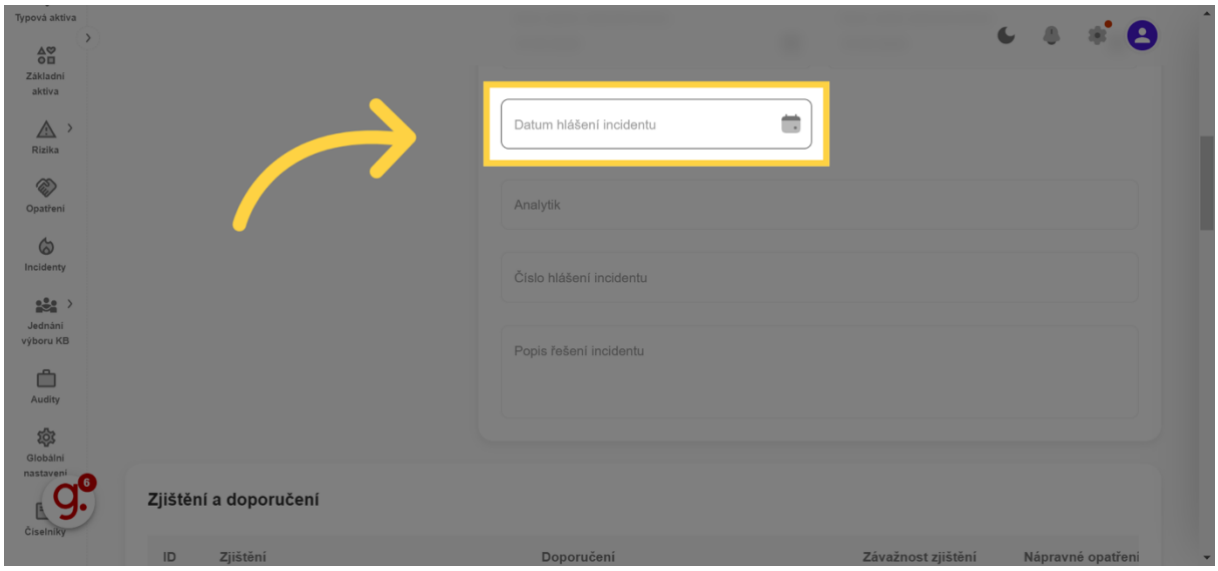
21. Typ

Můžete si všimnout, že Typ případu byl automaticky změněn na Incident. Tuto klasifikaci nelze měnit.



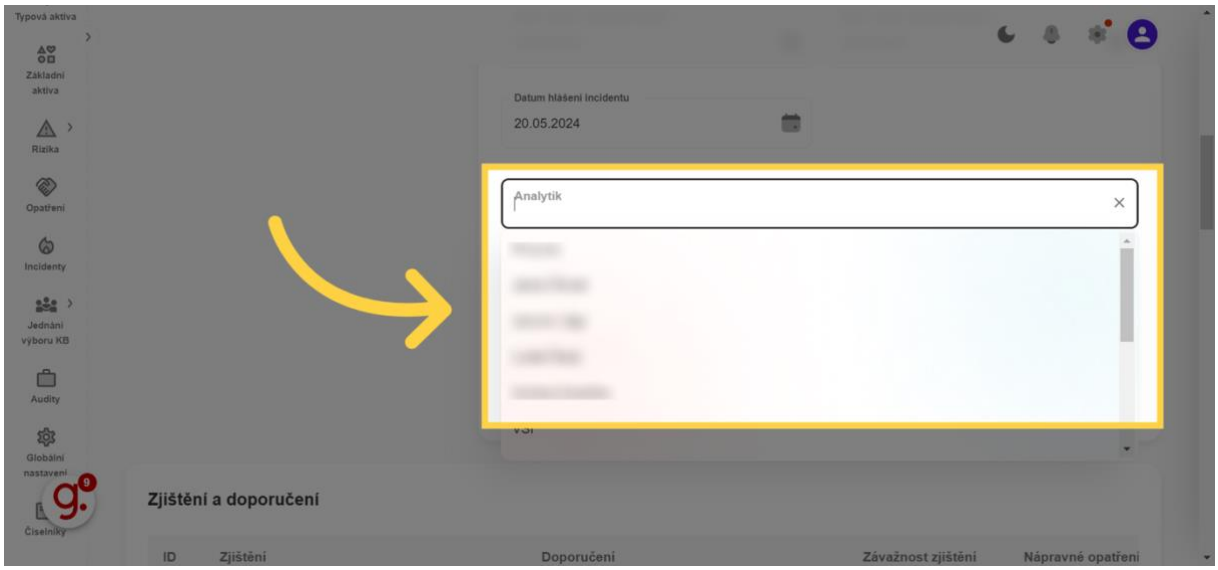
22. Datum hlášení

Jestliže vznikla povinnost incident nahlásit, je potřeba zaznamenat přesné datum nahlášení. Pokud je datum vyplněno, automaticky se přepíše hodnota položky Hlášení incidentu na "Incident byl nahlášen".



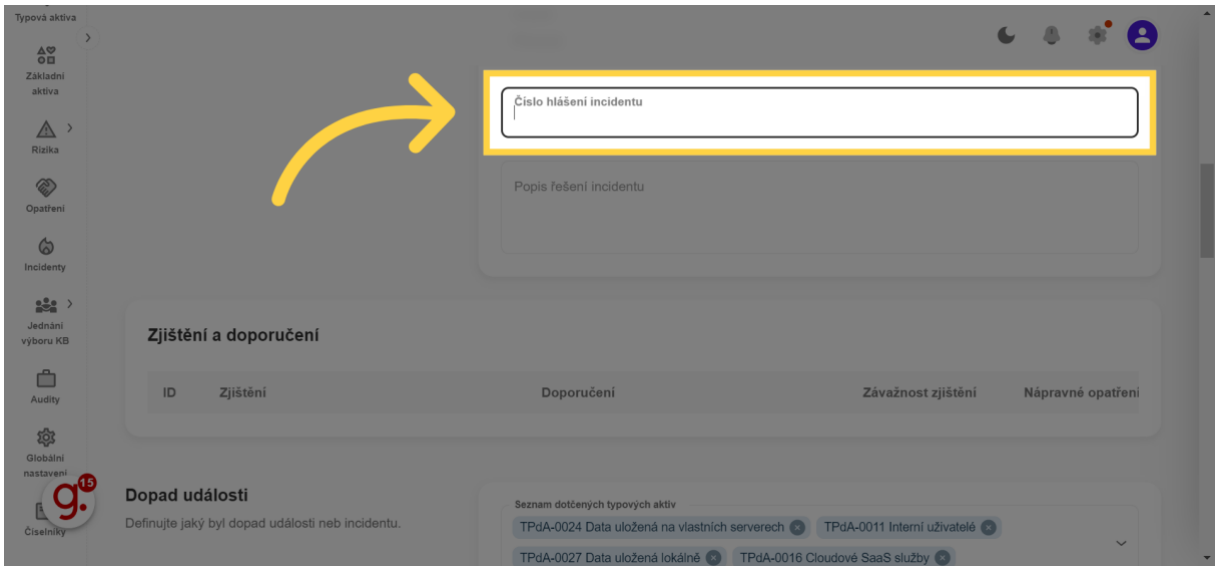
23. Analytik

Do políčka "Analytik" zapište osobu, která je odpovědná za vyhodnocení incidentu a jeho záznam v systému MoyaKybeon. Našeptávač navrhuje naposledy použitá jména, můžete ale zapsat jakékoli jméno.



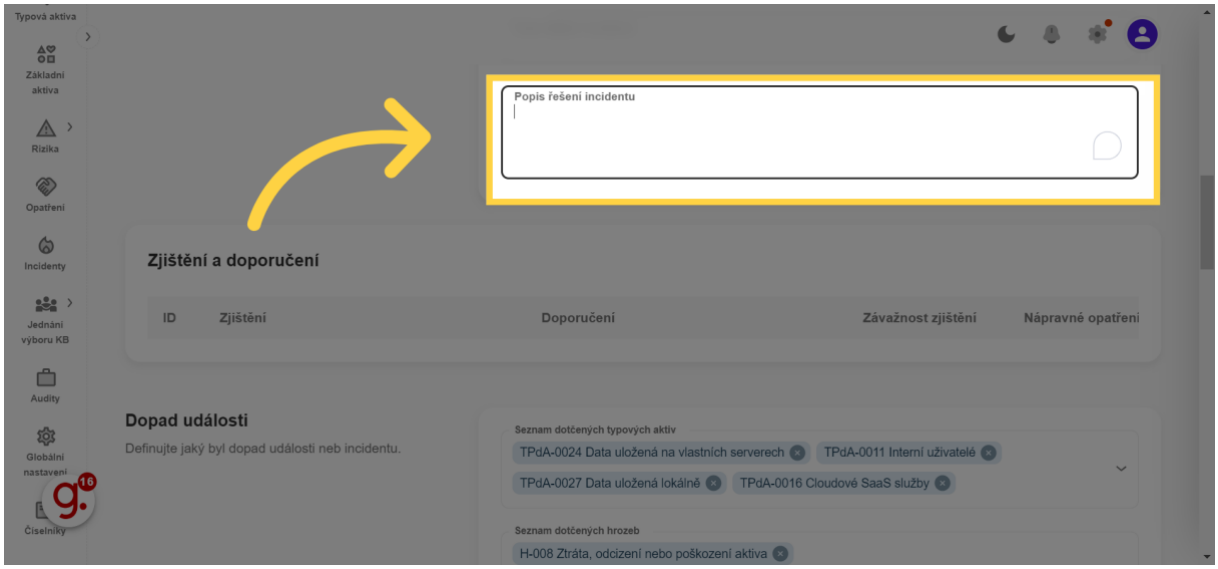
24. Číslo hlášení

Dále si zapište interní spisové číslo, pod kterým byl incident nahlášen.



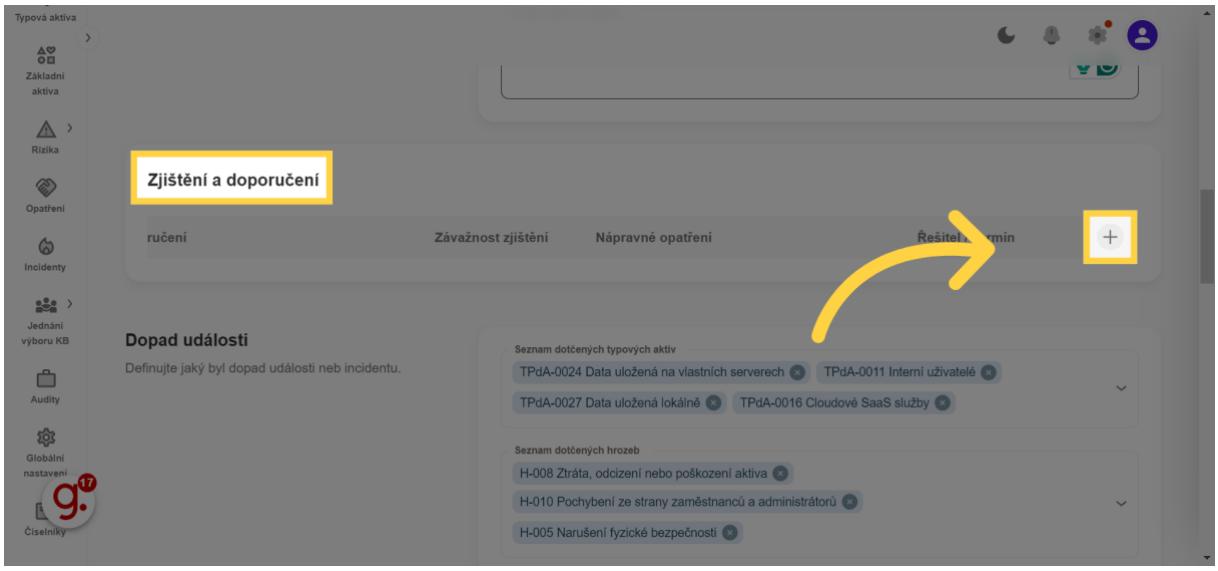
25. Popis řešení

Popište, jak byl incident řešen.



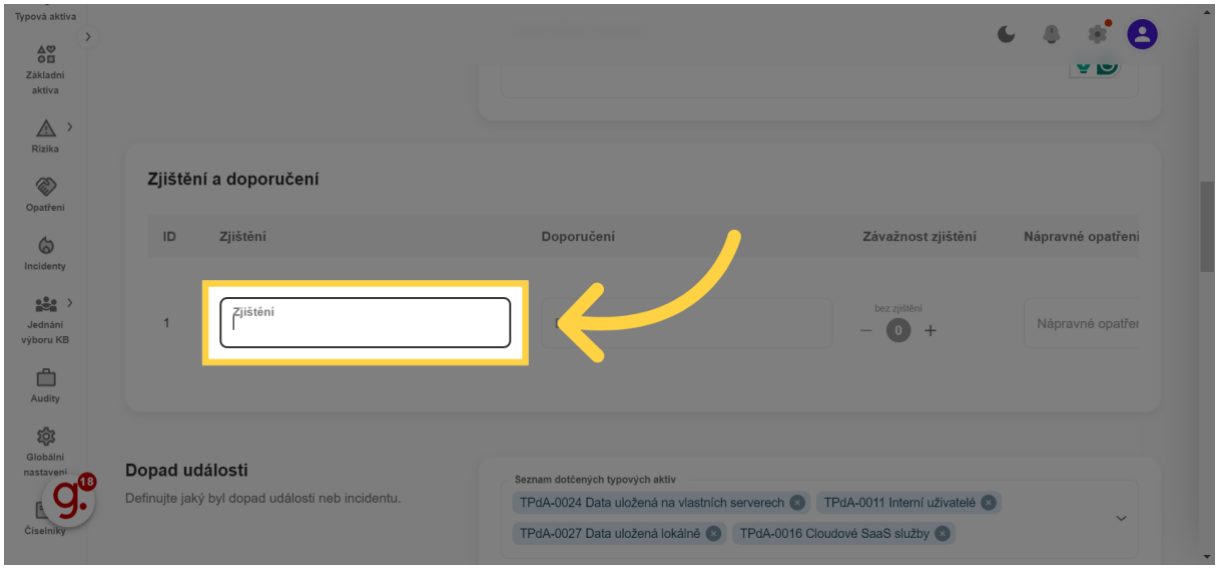
26. Zjištění a doporučení

Také je potřeba zaznamenat všechna související zjištění a doporučení. Pro zadání nové položky klikněte na "+".



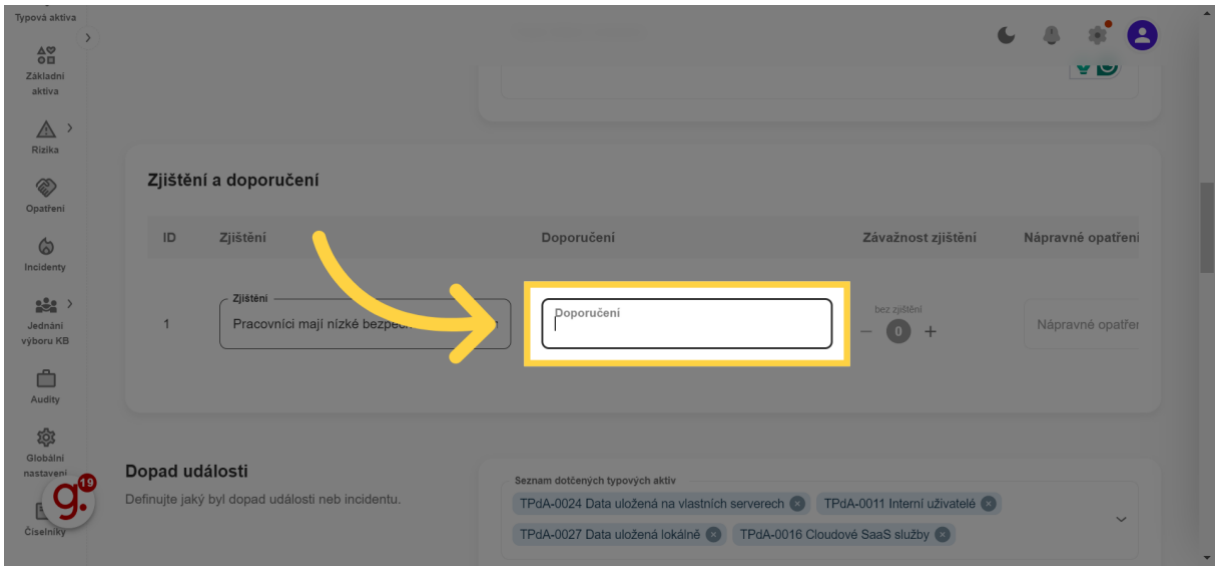
27. Zjištění

Stručně popište zjištění.



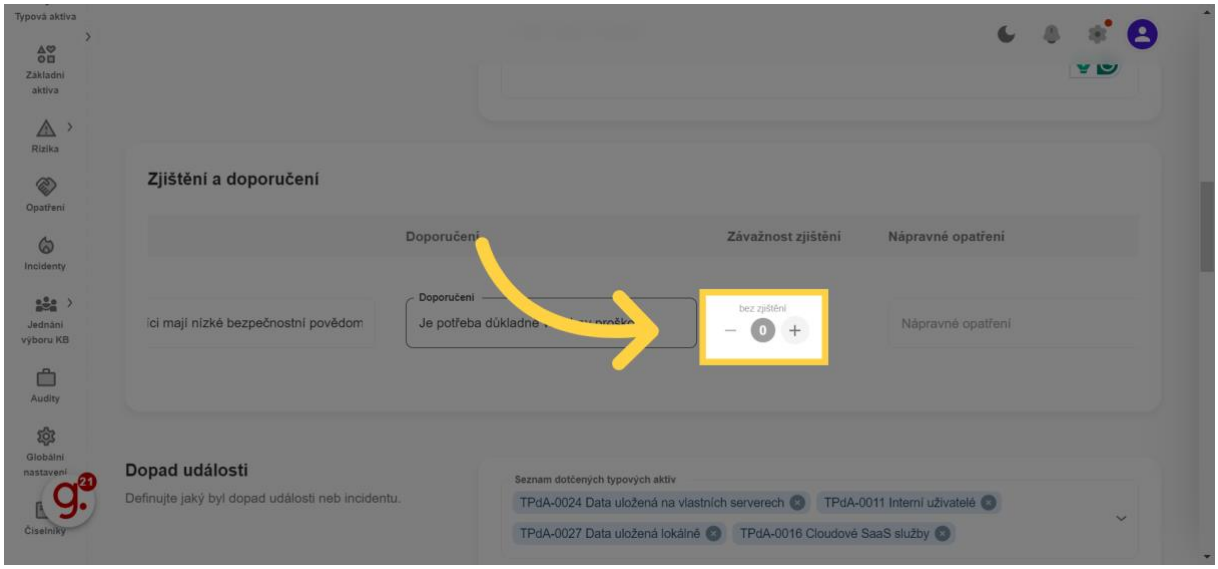
28. Doporučení

A následně doplňte stručný popis doporučení.



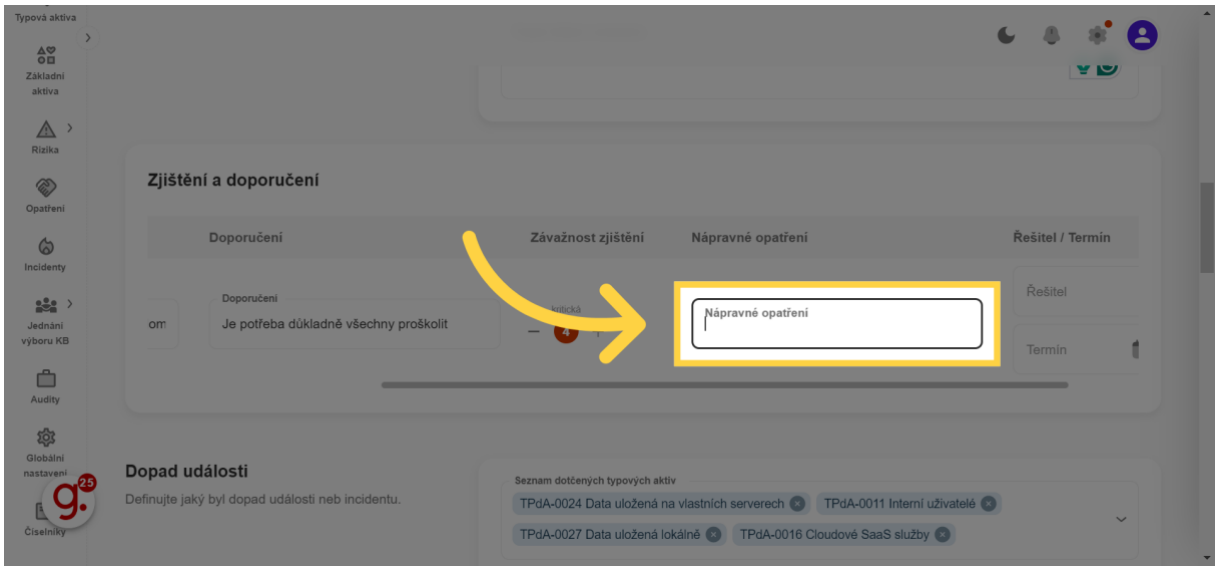
29. Závažnost

Pomocí plus a mínus nastavte závažnost zjištění.



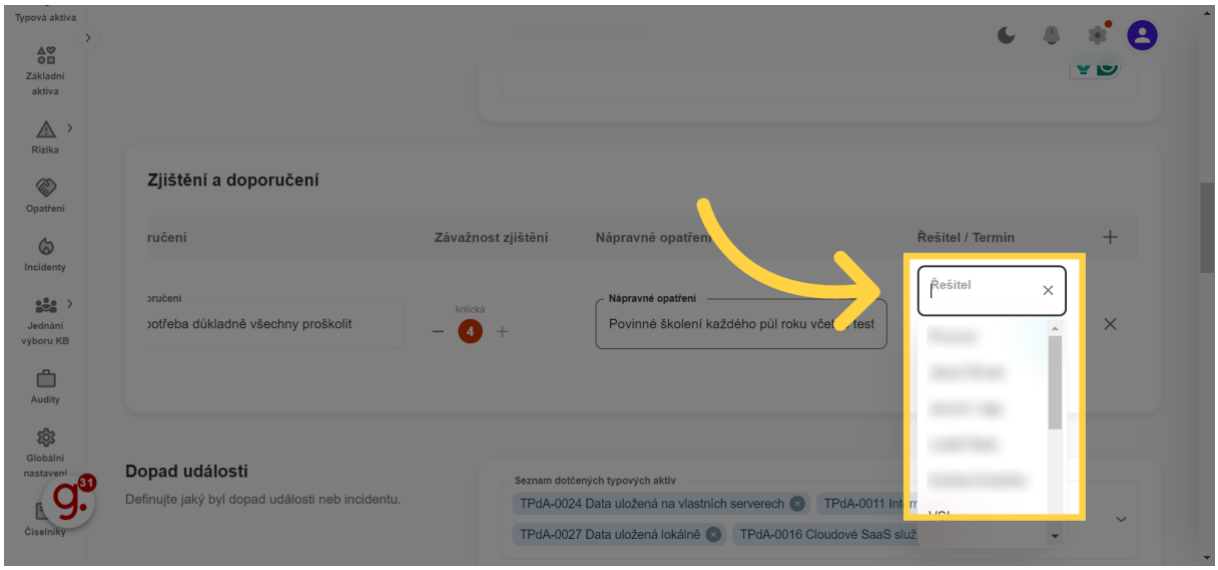
30. Nápravné opatření

Popište navrhované nápravné opatření.



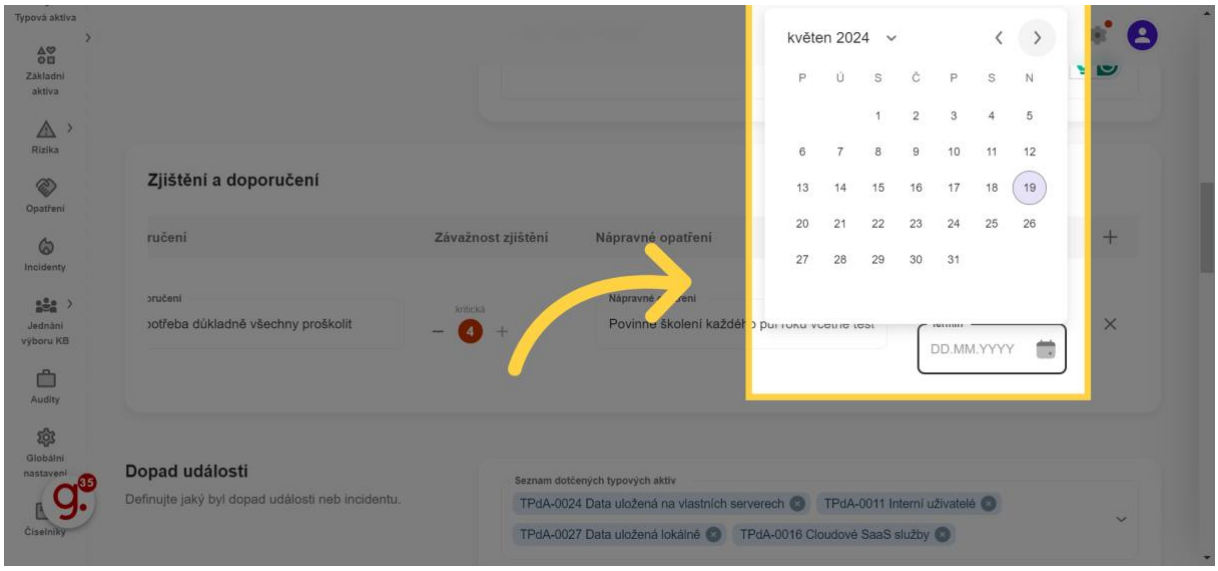
31. Řešitel

Zadejte, kdo má být za realizaci opatření zodpovědný. Automaticky se nabízí seznam osob, které byly v minulosti zadány, můžete ale vyplnit i novou osobu.



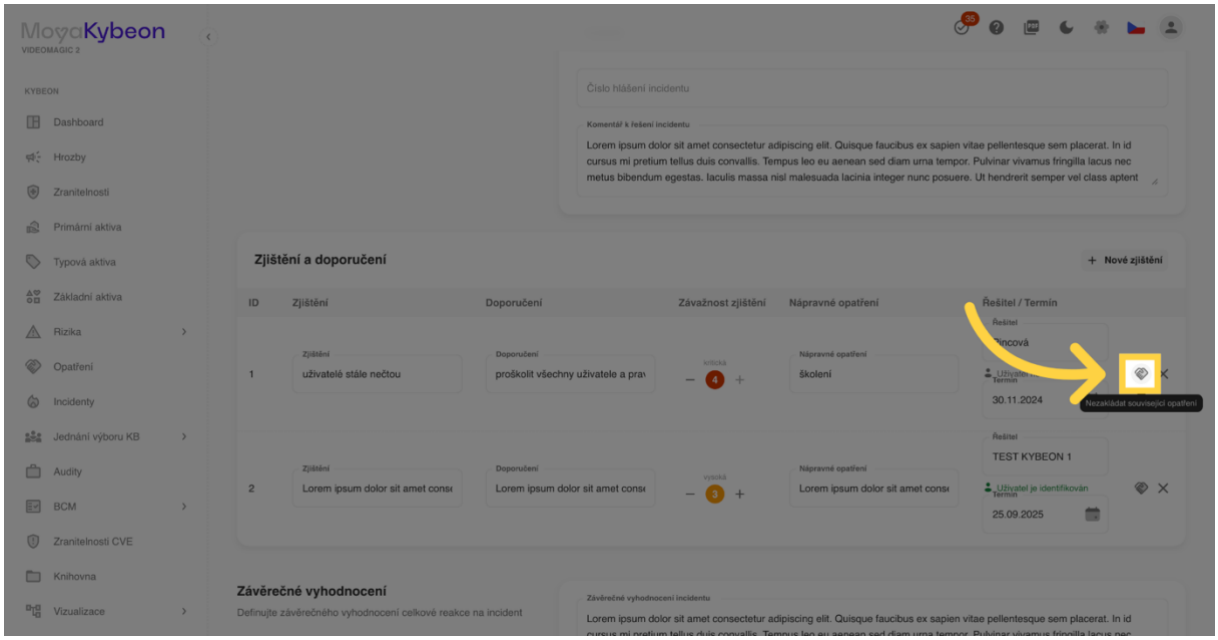
32. Datum

Doporučujeme také doplnit, do kdy má být opatření realizováno.



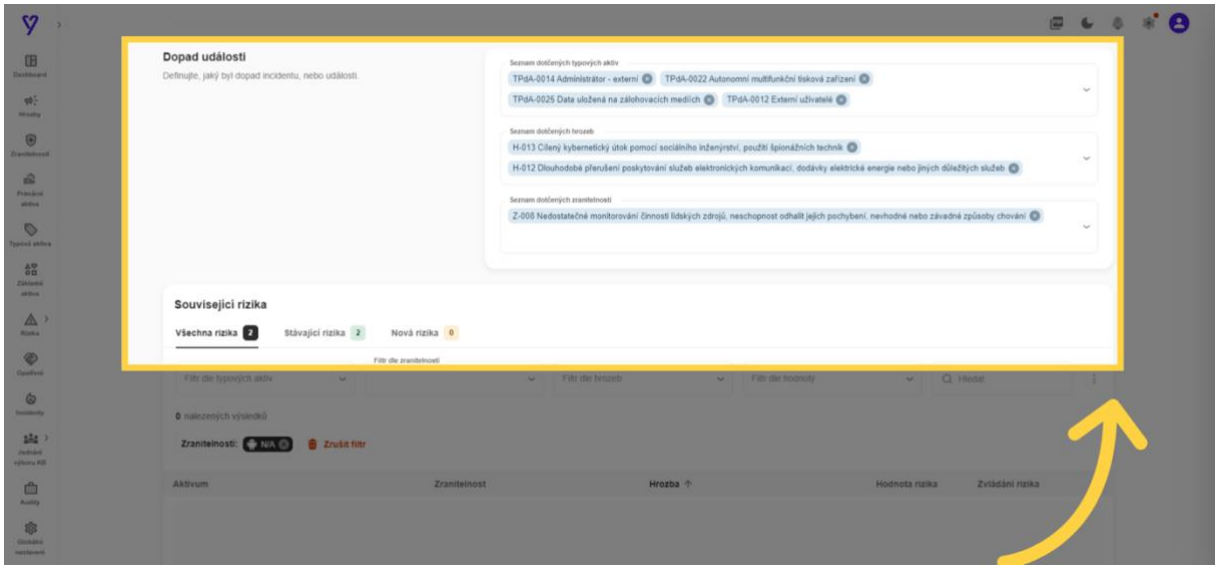
33. Založení opatření

Zaškrtnutím této ikony můžete automaticky založit dané opatření v katalogu opatření.



34. Dopad události

Před dokončením je potřeba zrevidovat dopad události - jakých typových aktiv, hrozeb a zranitelností se incident dotkl a jaká jsou související rizika.



35. Dokončení

Kliknutím na Dokončit uzavřete zpracování incidentu v aplikaci MoyaKybeon.