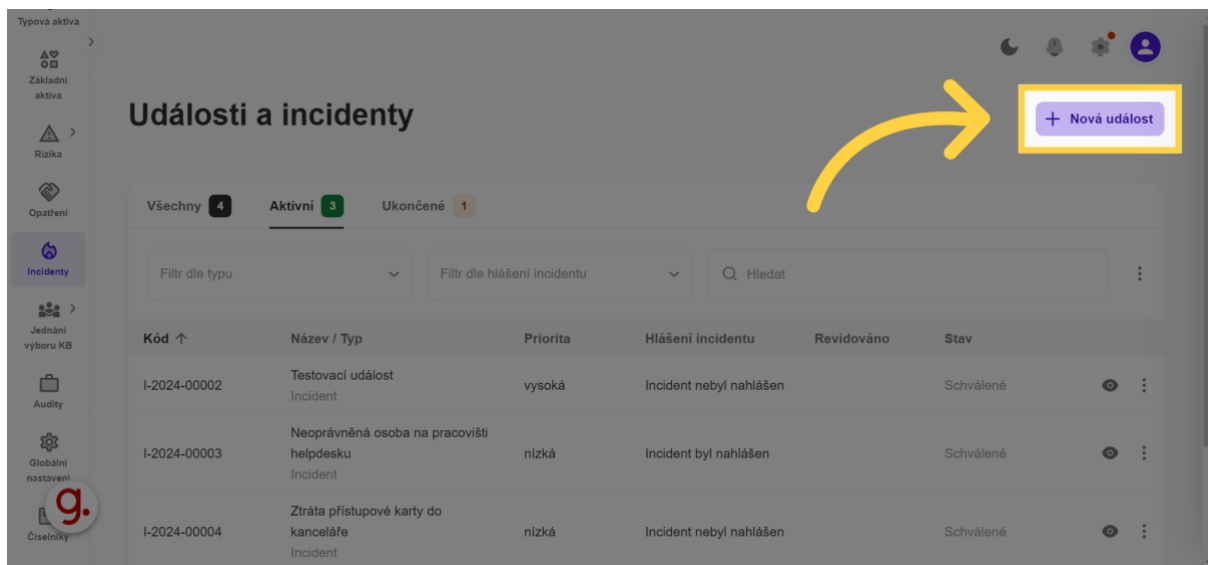


Události a incidenty

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.

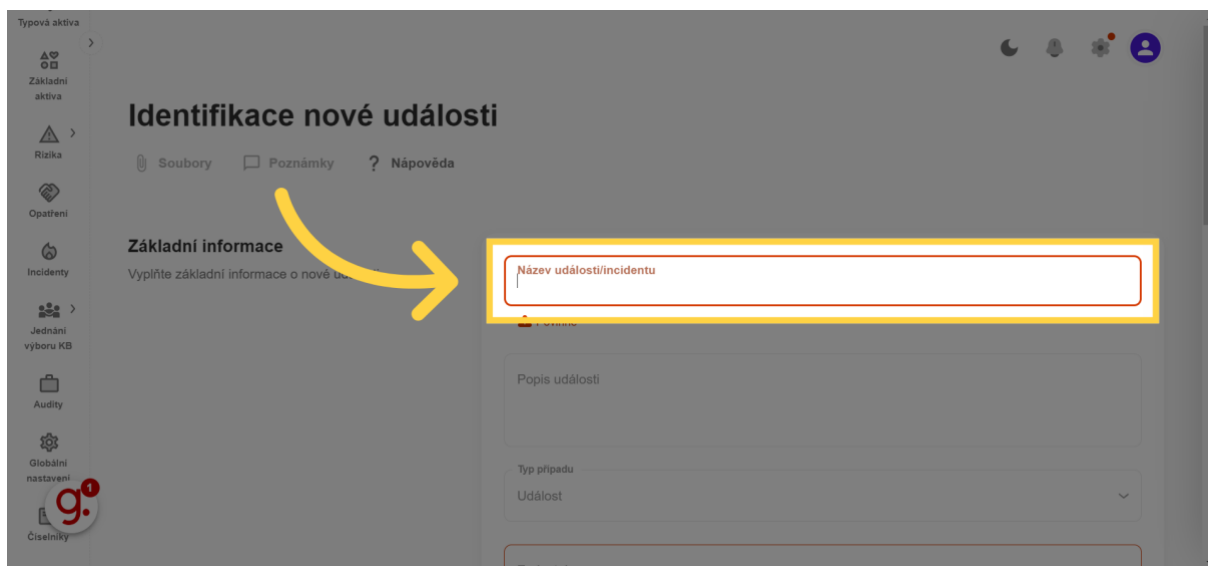
1. Nová událost

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



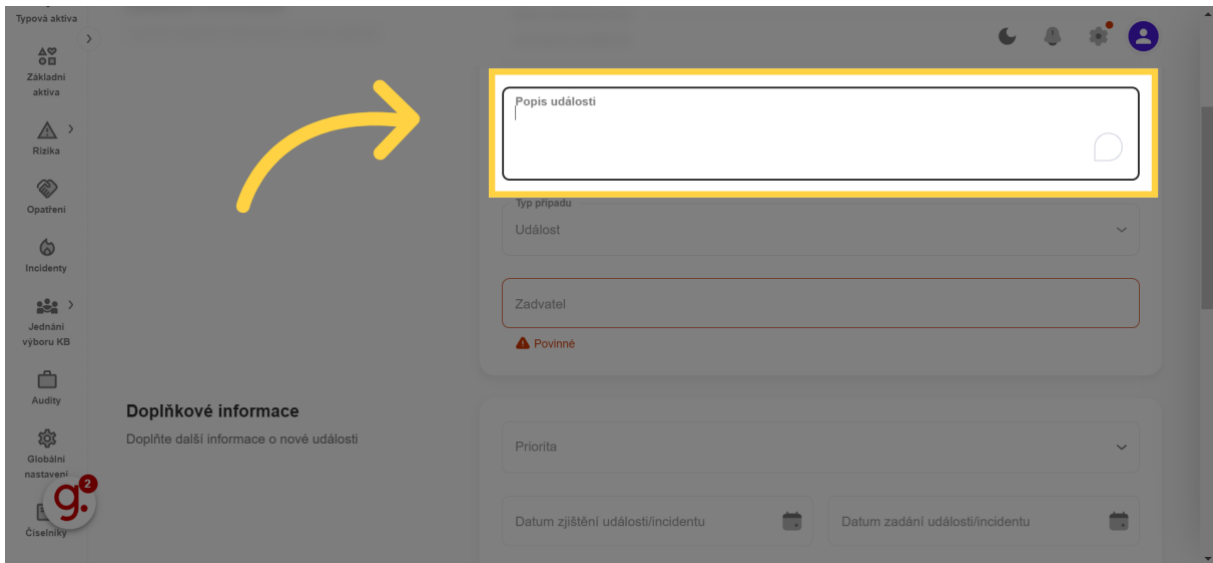
2. Název

Zadejte jednoznačné a jasné pojmenování nové události.



3. Popis

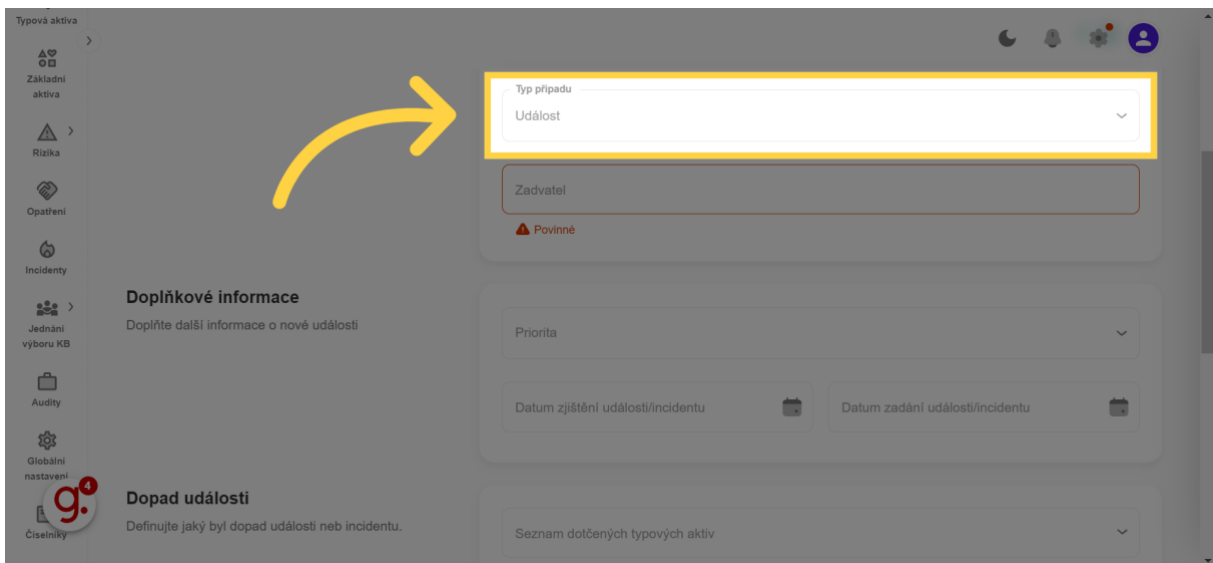
Vyplňte dostatečně podrobný slovní popis, který doplňuje název záznamu o informace důležité pro správné pochopení, co záznam reprezentuje.



The screenshot shows the 'Typová aktiva' (Typical Assets) form in the Moya Kybeon system. A yellow arrow points to the 'Popis události' (Event Description) text area, which is highlighted with a yellow border. The form includes a sidebar with navigation icons for 'Základní aktiva', 'Rizika', 'Opatření', 'Incidenty', 'Jednání', 'výboru KB', 'Audity', 'Globální nastavení', and 'Číselníky'. The main form fields include 'Typ případu' (Case Type) set to 'Událost' (Event), 'Zadavatel' (Requester), 'Priorita' (Priority), 'Datum zjištění události/incidentu' (Date of discovery), and 'Datum zadání události/incidentu' (Date of submission). A red 'Povinné' (Mandatory) icon is next to the 'Zadavatel' field.

4. Událost

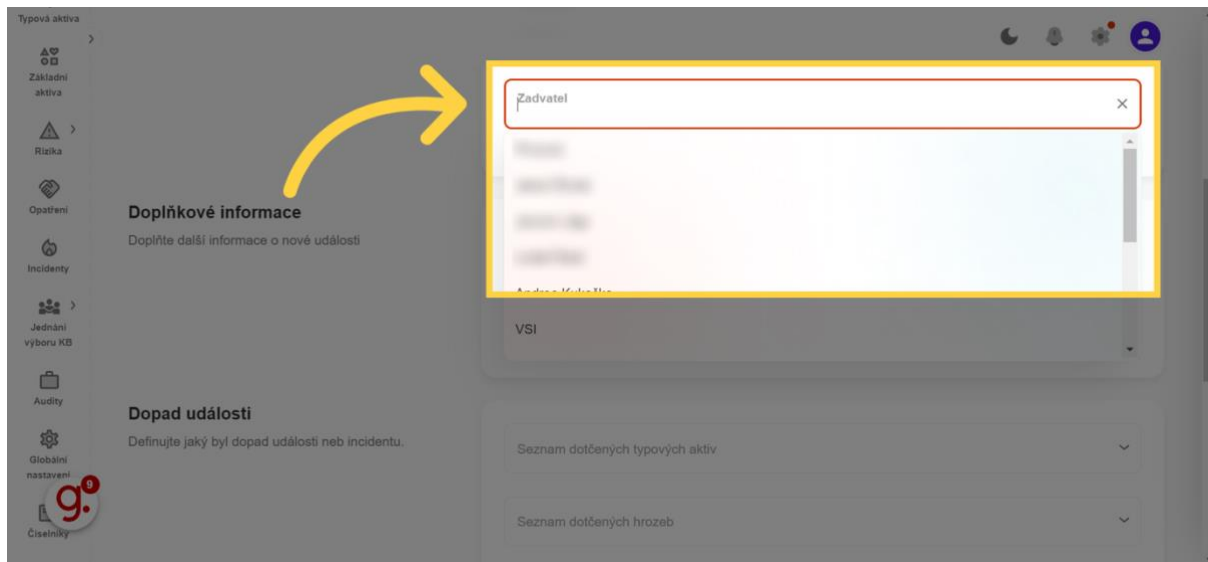
Při zadávání je případ automaticky klasifikován jako událost.



The screenshot shows the same 'Typová aktiva' form, but with the 'Typ případu' (Case Type) dropdown menu highlighted by a yellow box and a yellow arrow. The dropdown is currently set to 'Událost' (Event). The form fields are identical to the previous screenshot, including the sidebar, 'Zadavatel', 'Priorita', and date fields. A red 'Povinné' (Mandatory) icon is also present next to the 'Zadavatel' field.

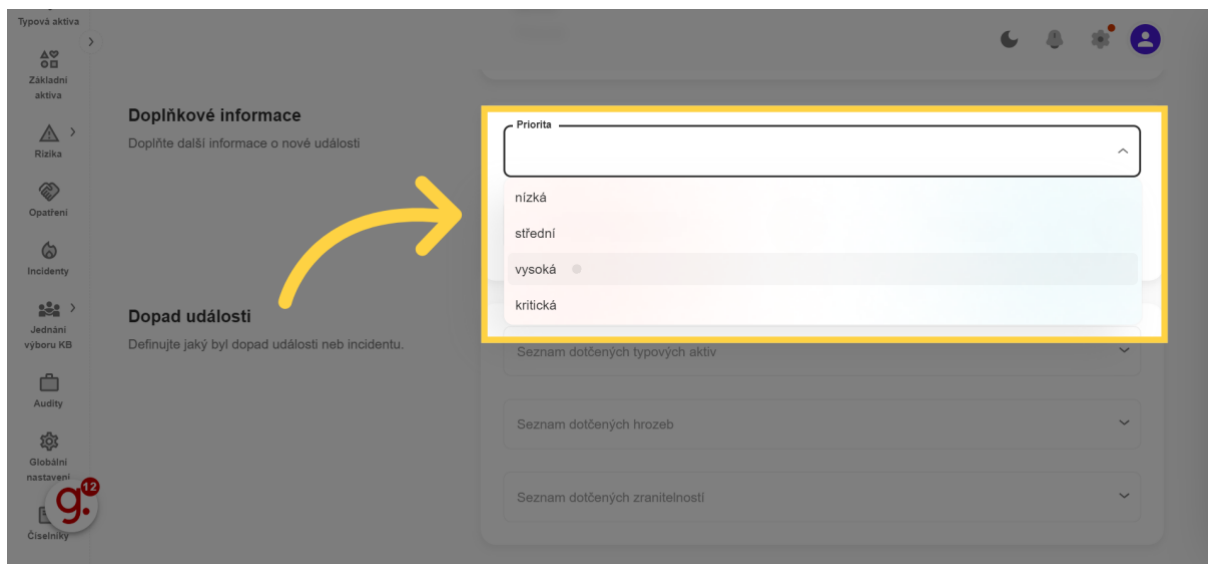
5. Zadavatel

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.



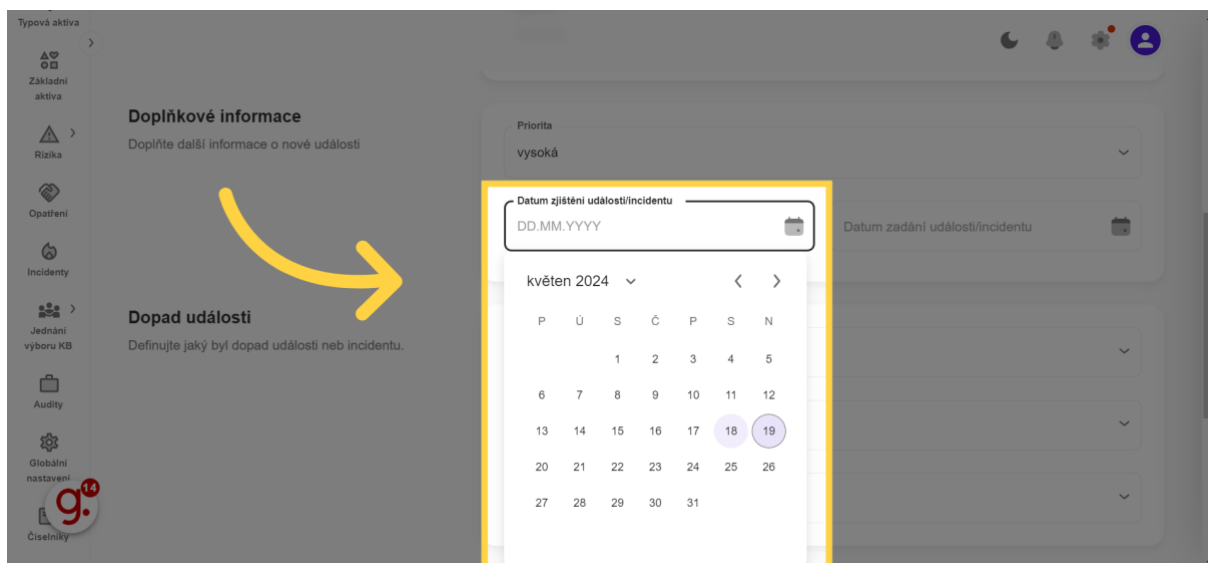
6. Priorita

Zadejte prioritu události.



7. Datum zjištění události

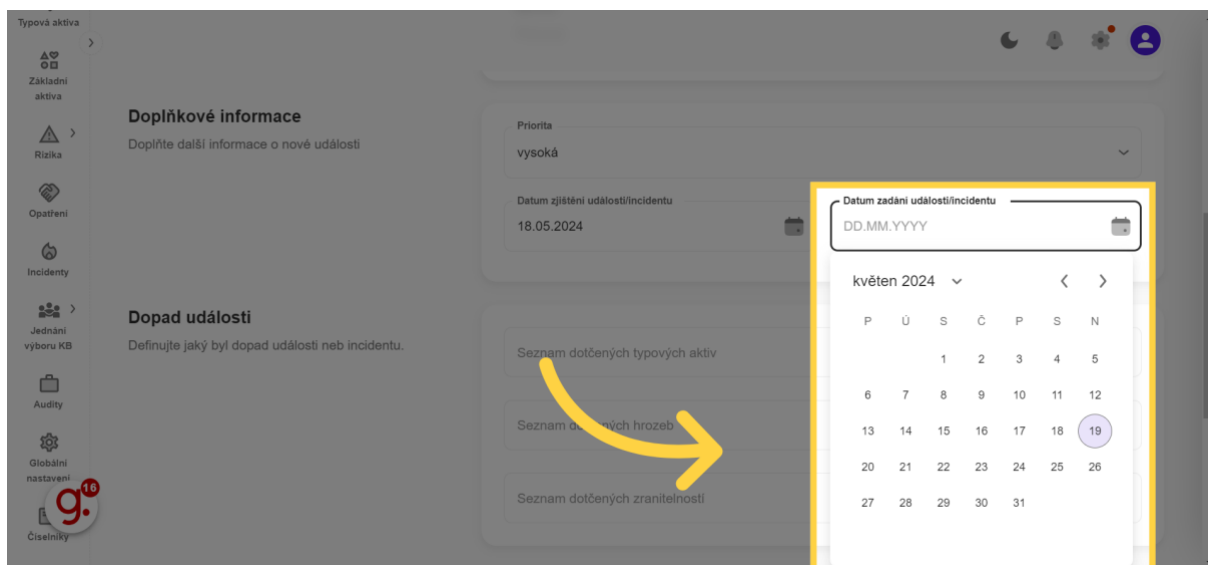
Zaznamenejte datum zjištění události.



The screenshot shows the MoyaKybeon interface with a sidebar on the left containing various icons and a main content area. The main content area has two sections: 'Doplňkové informace' (Additional information) and 'Dopad události' (Impact of the incident). The 'Doplňkové informace' section has a sub-section 'Datum zjištění události/incidentu' (Date of discovery of the incident) with a date picker. The date picker is open, showing a calendar for May 2024. The date 18.05.2024 is selected. A yellow arrow points to the date picker.

8. Datum zadání do MoyaKybeon

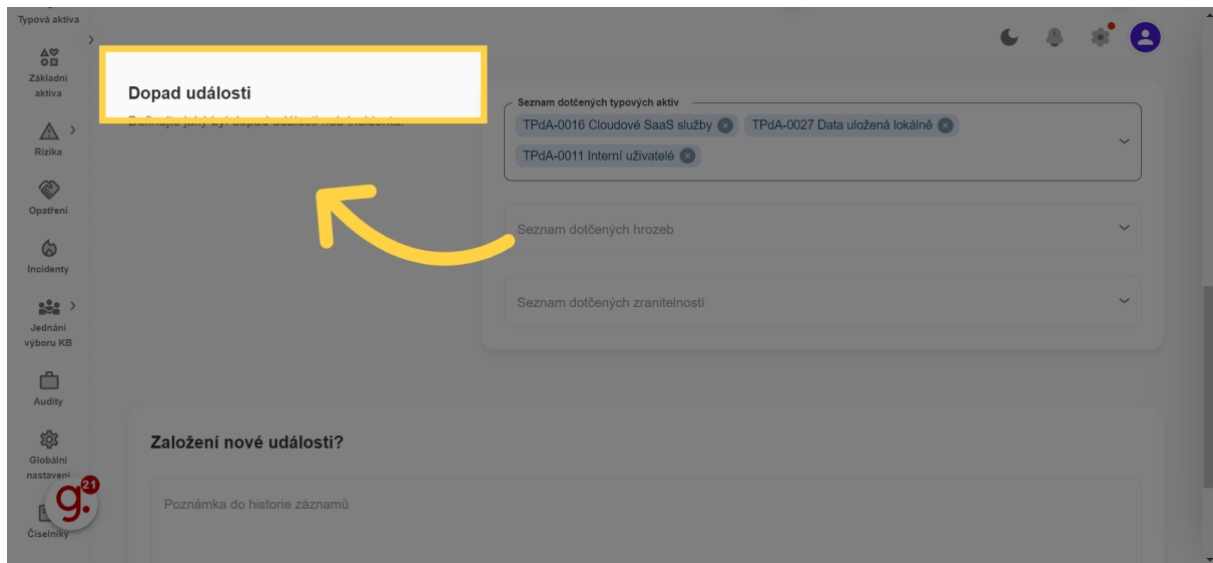
A také datum zadání do systému MoyaKybeon.



The screenshot shows the MoyaKybeon interface with a sidebar on the left containing various icons and a main content area. The main content area has two sections: 'Doplňkové informace' (Additional information) and 'Dopad události' (Impact of the incident). The 'Doplňkové informace' section has a sub-section 'Datum zadání události/incidentu' (Date of entry into the system) with a date picker. The date picker is open, showing a calendar for May 2024. The date 19.05.2024 is selected. A yellow arrow points to the date picker.

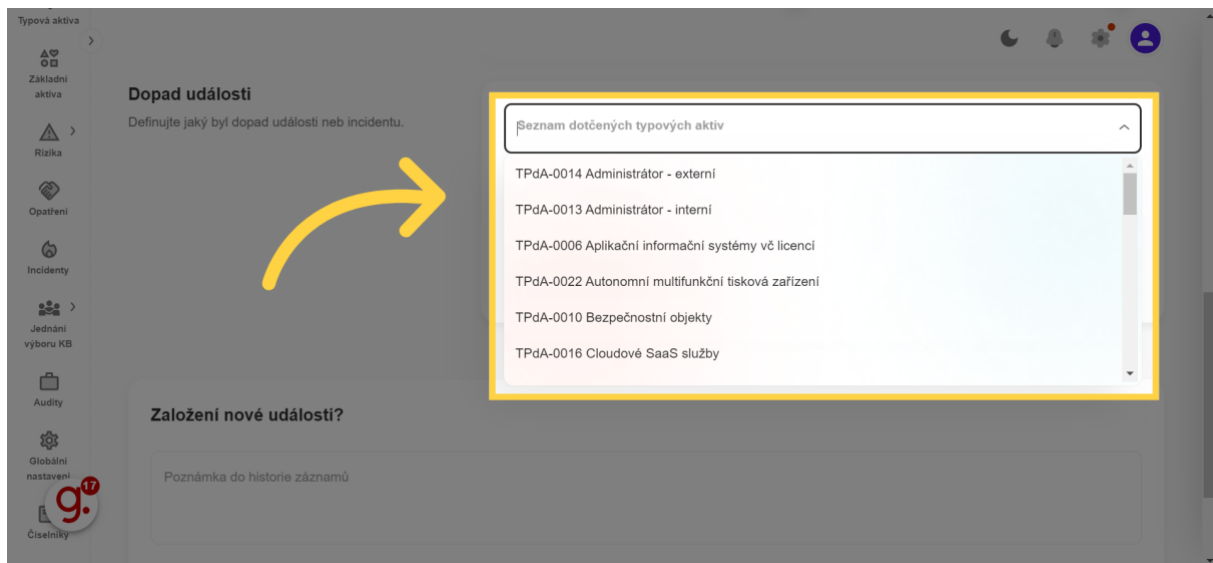
9. Dopad

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



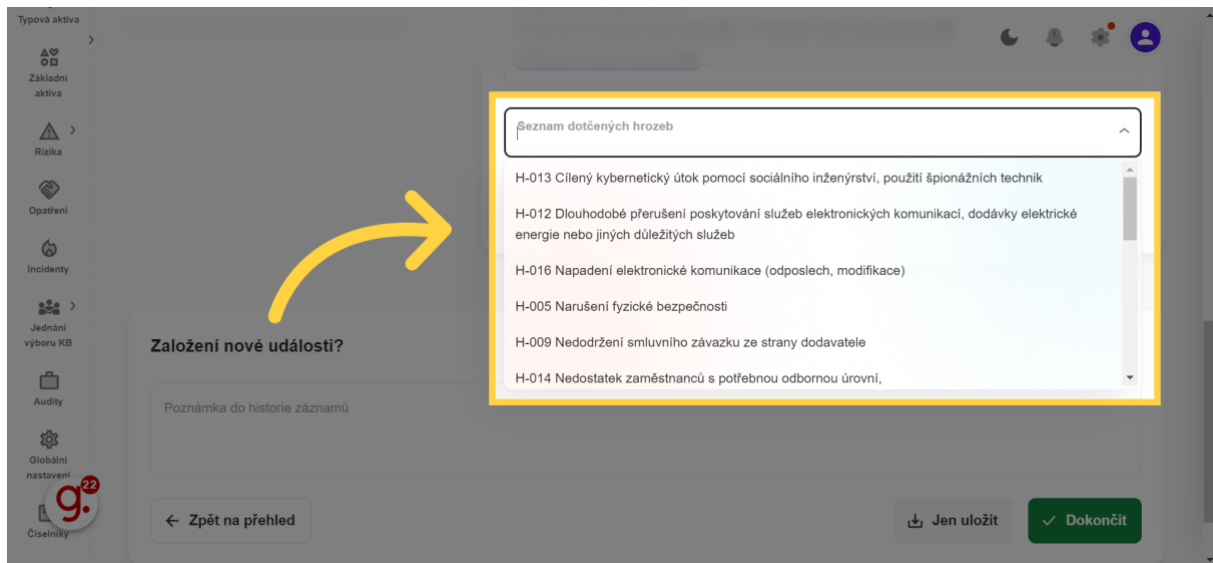
10. Typová aktiva

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



11. Hrozby

Vyberte všechny hrozby, které při bezpečnostní události působily.



Typová aktiva

Základní aktiva

Rizika

Opatření

Incidenty

Jednání výboru KB

Audity

Globální nastavení

Číselníky

9.22

Založení nové události?

Poznámka do historie záznamů

← Zpět na přehled

Jen uložit

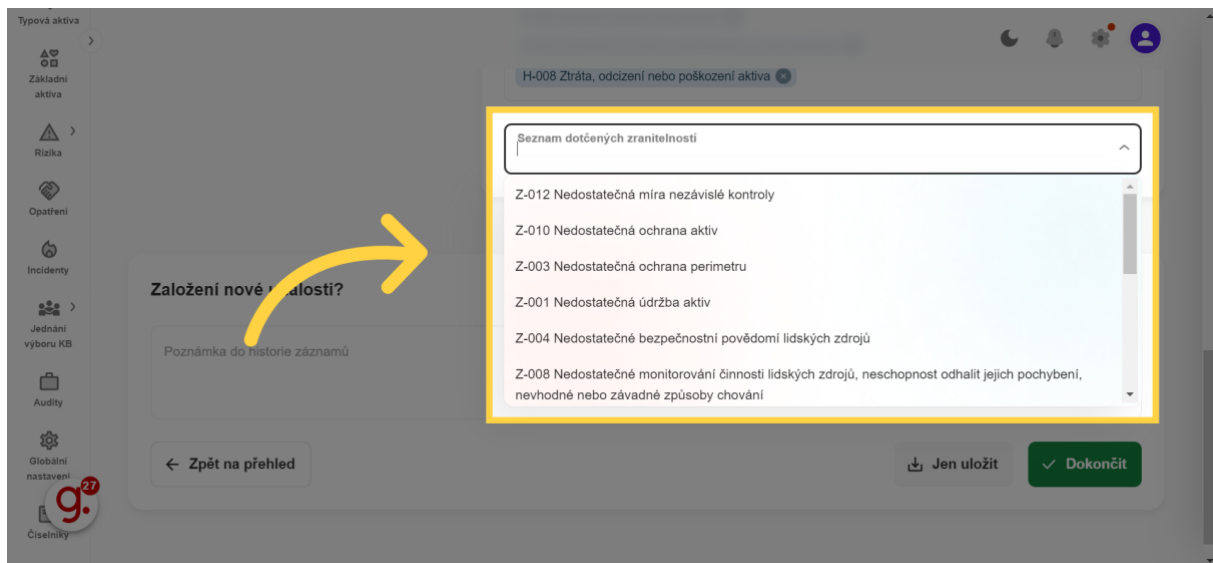
✓ Dokončit

Seznam dotčených hrozeb

- H-013 Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik
- H-012 Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb
- H-016 Napadení elektronické komunikace (odposlech, modifikace)
- H-005 Narušení fyzické bezpečnosti
- H-009 Nedodržení smluvního závazku ze strany dodavatele
- H-014 Nedostatek zaměstnanců s potřebnou odbornou úrovní,

12. Zranitelnosti

A také vyberte všechny zranitelnosti, které bezpečnostní událost umožnily.



Typová aktiva

Základní aktiva

Rizika

Opatření

Incidenty

Jednání výboru KB

Audity

Globální nastavení

Číselníky

9.27

Založení nové události?

Poznámka do historie záznamů

← Zpět na přehled

Jen uložit

✓ Dokončit

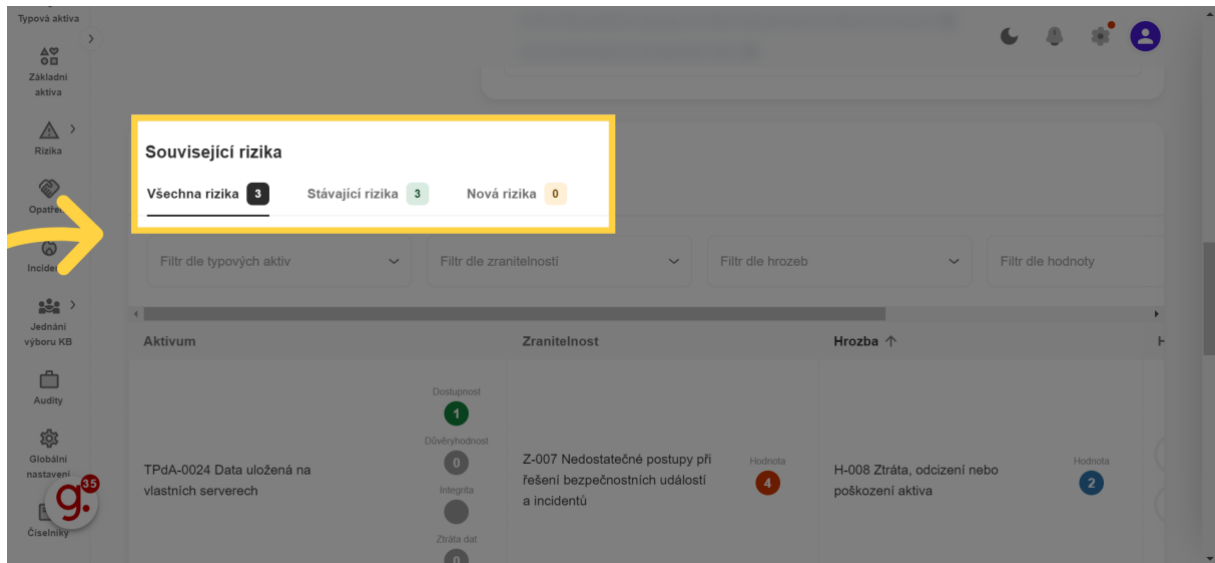
H-008 Ztráta, odcizení nebo poškození aktiva

Seznam dotčených zranitelností

- Z-012 Nedostatečná míra nezávislé kontroly
- Z-010 Nedostatečná ochrana aktiv
- Z-003 Nedostatečná ochrana perimetru
- Z-001 Nedostatečná údržba aktiv
- Z-004 Nedostatečné bezpečnostní povědomí lidských zdrojů
- Z-008 Nedostatečné monitorování činnosti lidských zdrojů, neschopnost odhalit jejich pochybení, nevhodné nebo závažné způsoby chování

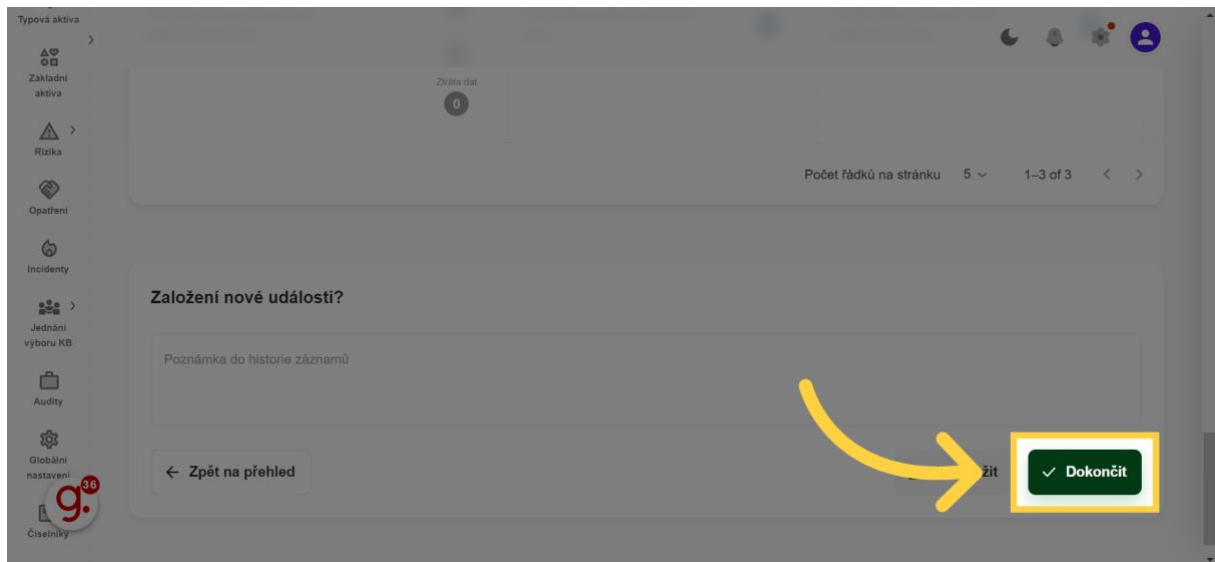
13. Rizika

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



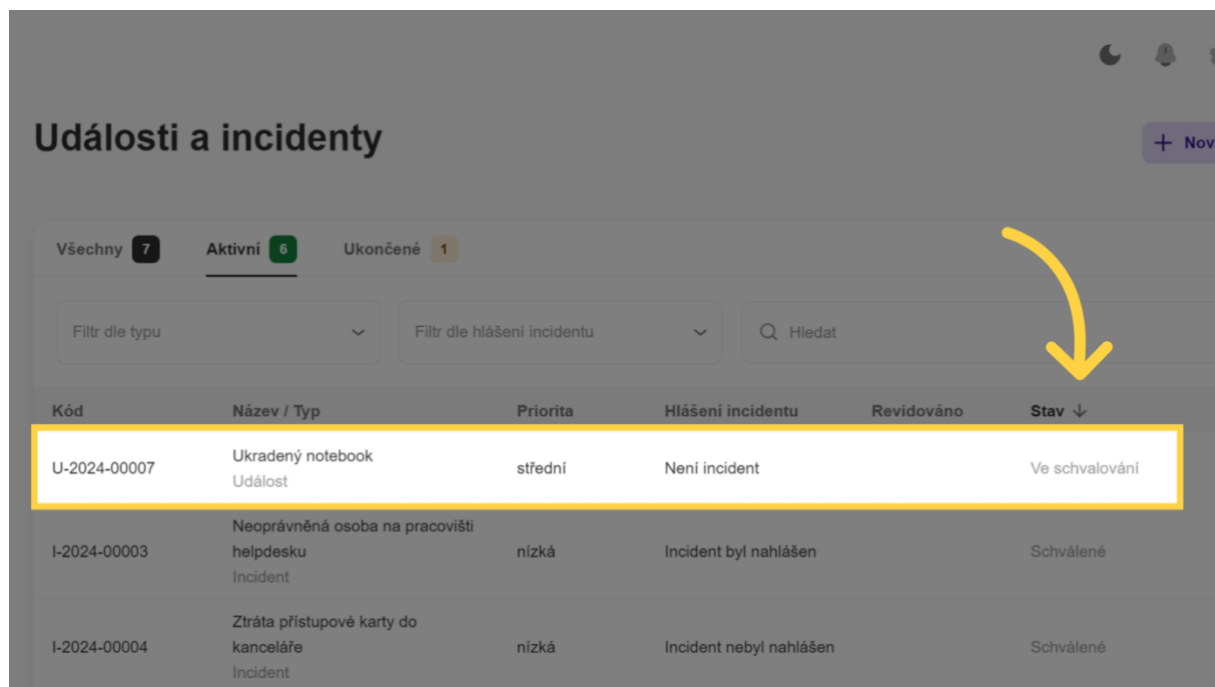
14. Dokončit 1

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

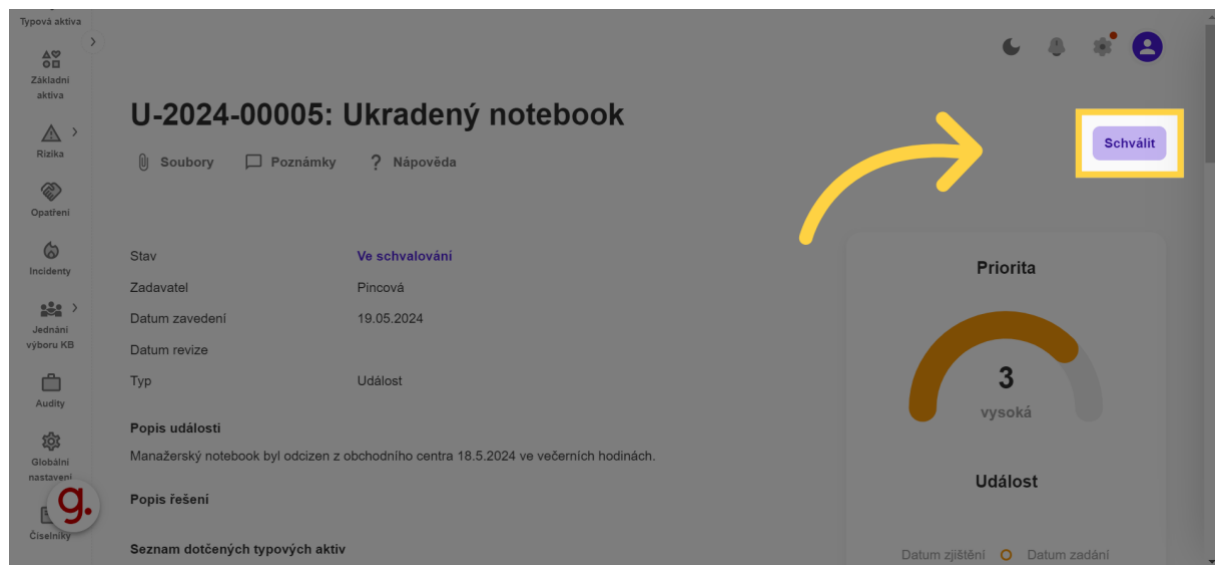
Každou novou událost je potřeba schválit a vyhodnotit.



Kód	Název / Typ	Priorita	Hlášení incidentu	Revidováno	Stav ↓
U-2024-00007	Ukradený notebook Událost	střední	Není incident		Ve schvalování
I-2024-00003	Neoprávněná osoba na pracovišti helpdesku Incident	nizká	Incident byl nahlášen		Schválené
I-2024-00004	Ztráta přístupové karty do kanceláře Incident	nizká	Incident nebyl nahlášen		Schválené

16. Schválení

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



U-2024-00005: Ukradený notebook

Soubory Poznámky Nápověda

Stav: **Ve schvalování**

Zadavatel: Pincová

Datum zavedení: 19.05.2024

Datum revize:

Typ: Událost

Popis události
Manažerský notebook byl odcizen z obchodního centra 18.5.2024 ve večerních hodinách.

Popis řešení

Seznam dotčených typových aktiv

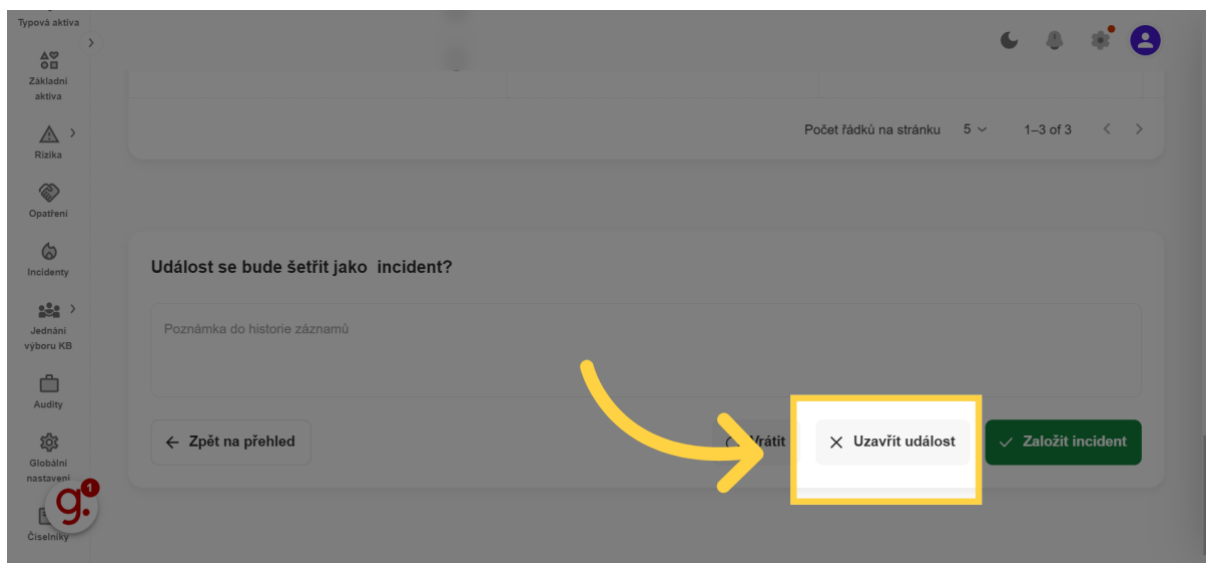
Priorita
3
vysoká

Událost

Datum zjištění Datum zadání

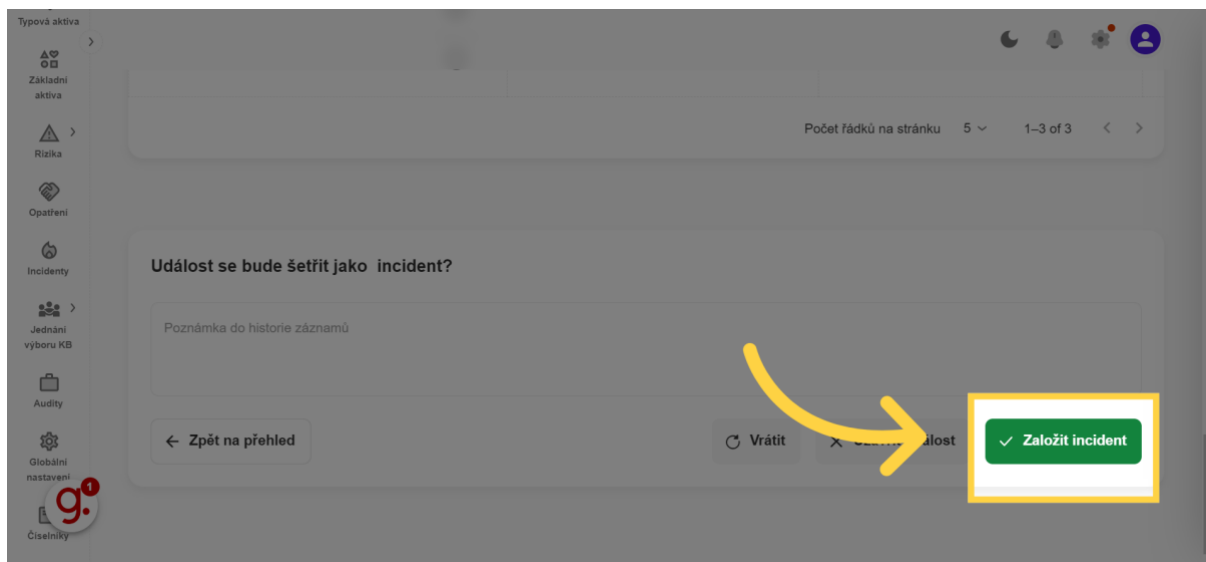
17. Uzavření

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



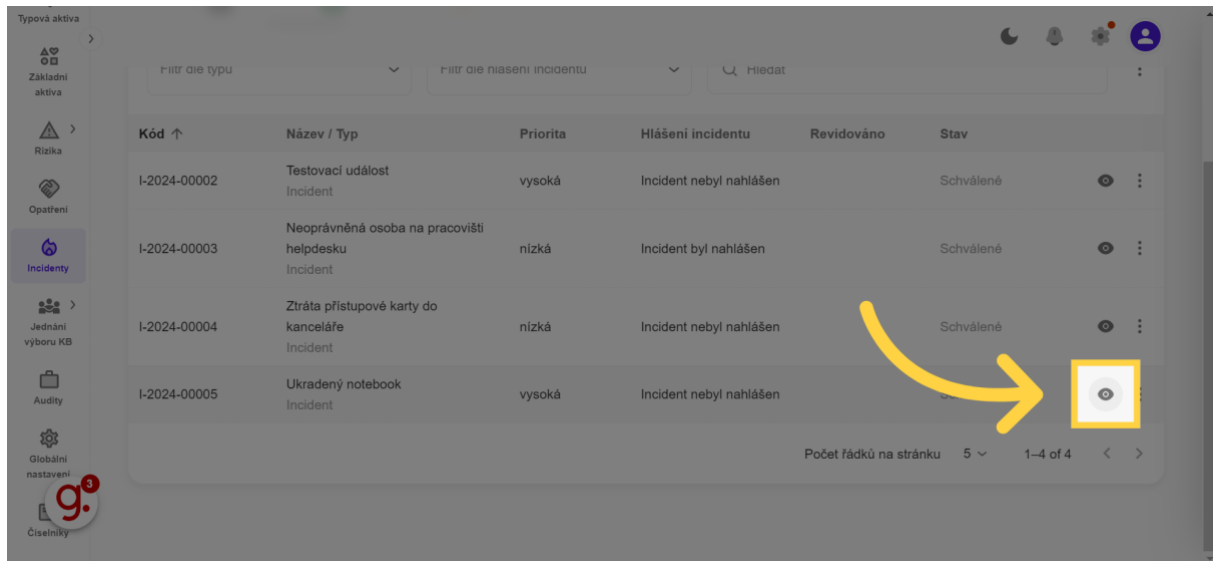
18. Založení incidentu

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



19. Detail

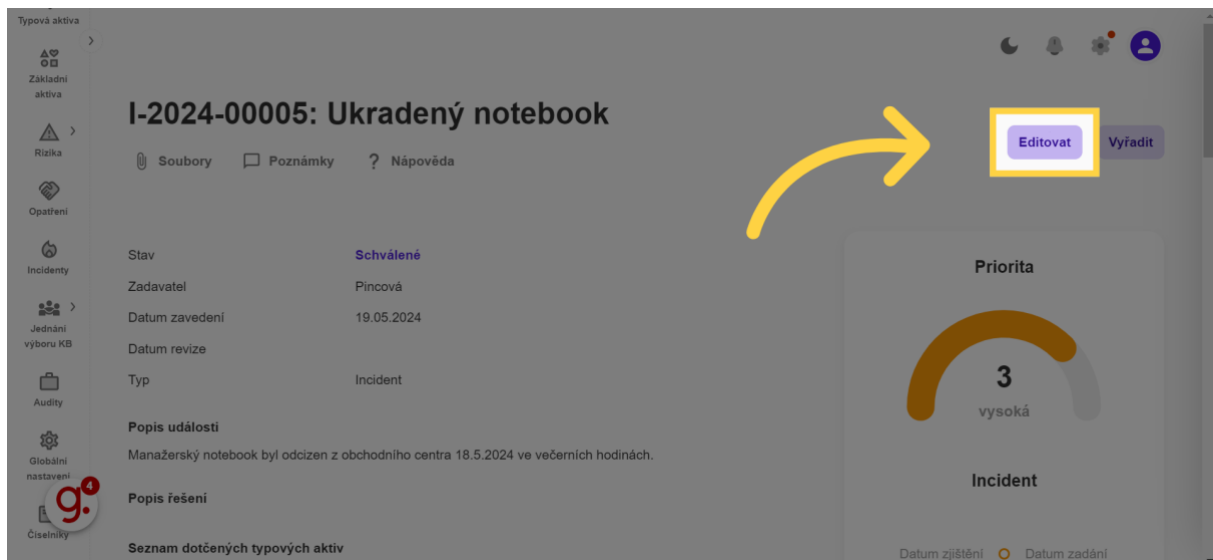
Pojďme se dále podívat, co je potřeba zaznamenat, pokud schvalovatel řekl, že je potřeba událost překlasifikovat na incident. Detaily incidentu si otevřete z přehledu.



Kód ↑	Název / Typ	Priorita	Hlášení incidentu	Revidováno	Stav	
I-2024-00002	Testovací událost Incident	vysoká	Incident nebyl nahlášen		Schválené	
I-2024-00003	Neoprávněná osoba na pracovišti helpdesku Incident	nízká	Incident byl nahlášen		Schválené	
I-2024-00004	Ztráta přístupové karty do kanceláře Incident	nízká	Incident nebyl nahlášen		Schválené	
I-2024-00005	Ukradený notebook Incident	vysoká	Incident nebyl nahlášen		Schválené	

20. Editace

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



I-2024-00005: Ukradený notebook

Soubory Poznámky Nápověda

Stav	Schválené
Zadavatel	Pincová
Datum zavedení	19.05.2024
Datum revize	
Typ	Incident

Popis události
Manažerský notebook byl odcizen z obchodního centra 18.5.2024 ve večerních hodinách.

Popis řešení

Seznam dotčených typových aktiv

Priorita

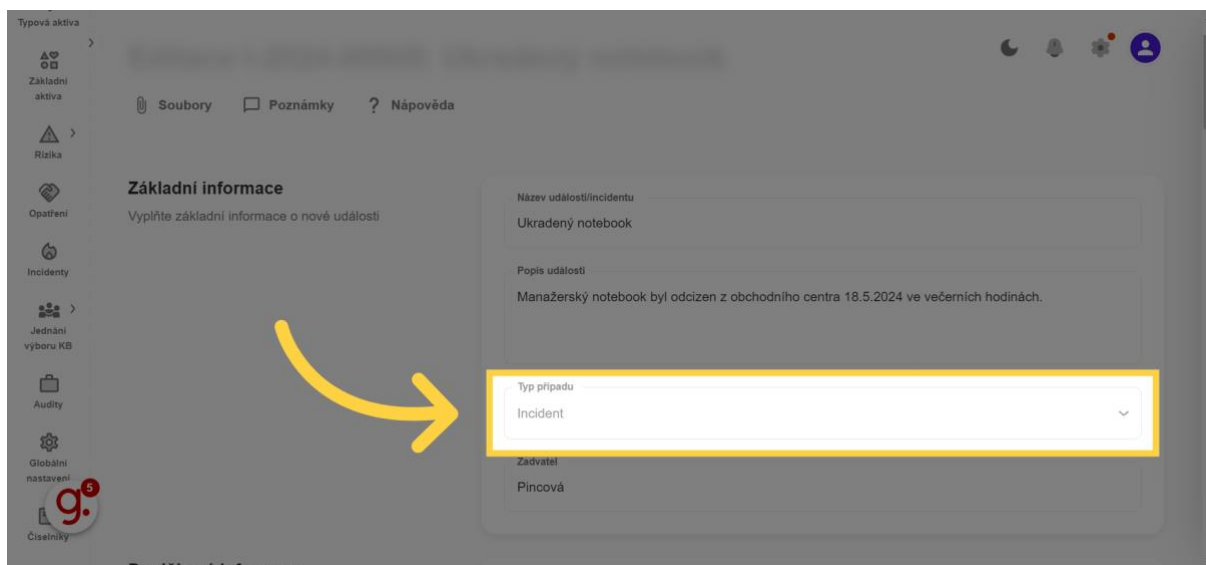
3
vysoká

Incident

Datum zjištění Datum zadání

21. Typ

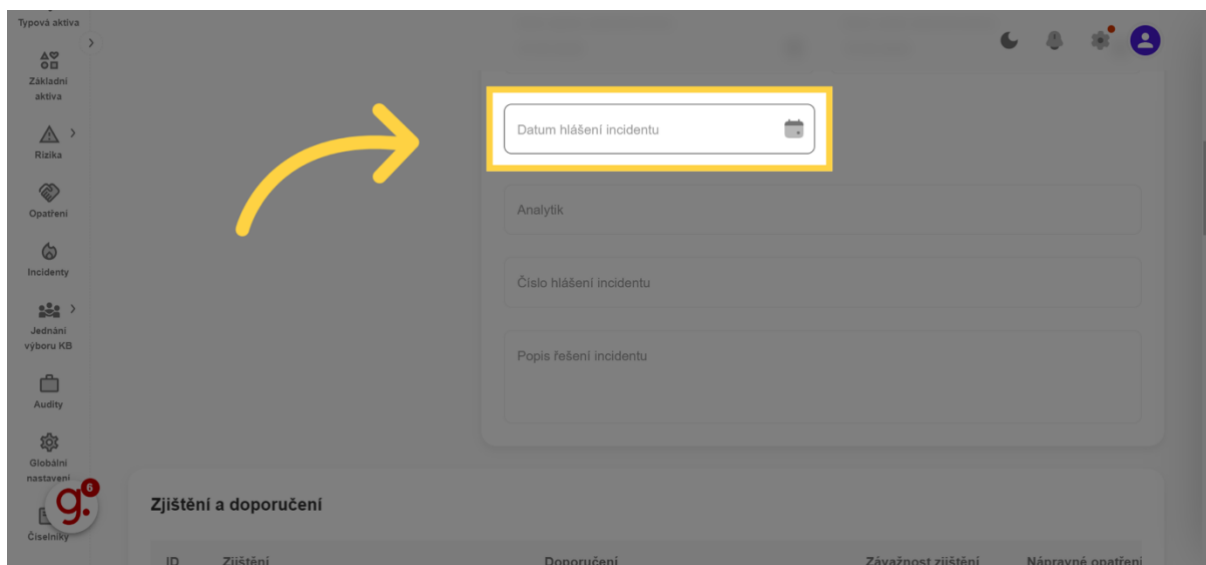
Můžete si všimnout, že Typ případu byl automaticky změněn na Incident. Tuto klasifikaci nelze měnit.



The screenshot shows the 'Základní informace' (Basic information) section of the MoyaKybeon interface. A yellow arrow points to the 'Typ případu' (Case type) dropdown menu, which is set to 'Incident'. The dropdown menu is highlighted with a yellow border. The 'Základní informace' section includes fields for 'Název události/incidentu' (Event/incident name), 'Popis události' (Event description), 'Zařaditel' (Assigner), and 'Přidělovatel' (Assignee). The 'Název události/incidentu' field contains the text 'Ukradený notebook' (Stolen notebook). The 'Popis události' field contains the text 'Manažerský notebook byl odcizen z obchodního centra 18.5.2024 ve večerních hodinách.' (Managerial notebook was stolen from the shopping center 18.5.2024 in the evening hours).

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 nhlášen".



The screenshot shows the 'Datum hlášení incidentu' (Incident report date) field in the MoyaKybeon interface. A yellow arrow points to the field, which is highlighted with a yellow border. The field is located in the 'Zjištění a doporučení' (Findings and recommendations) section. Below the 'Datum hlášení incidentu' field are fields for 'Analytik' (Analyst), 'Číslo hlášení incidentu' (Incident report number), and 'Popis řešení incidentu' (Incident resolution description). The 'Zjištění a doporučení' section also includes a table with columns: ID, Zjištění (Findings), Doporučení (Recommendations), Závažnost zjištění (Severity of findings), and Nápravné opatření (Corrective action).

23. Analytik

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

The screenshot shows the MoyaKybeon interface. On the left is a sidebar with icons for 'Základní aktiva', 'Rizika', 'Opatření', 'Incidenty', 'Jednání výboru KB', 'Audity', 'Globální nastavení', and 'Číslenky'. The main area has a header 'Datum hlášení Incidentu' with the date '20.05.2024'. Below this is a form with a field labeled 'Analytik' which is highlighted with a yellow box. A yellow arrow points from the left towards this field. Below the 'Analytik' field is a section titled 'Zjištění a doporučení' with a table that has columns: 'ID', 'Zjištění', 'Doporučení', 'Závažnost zjištění', and 'Nápravné opatření'.

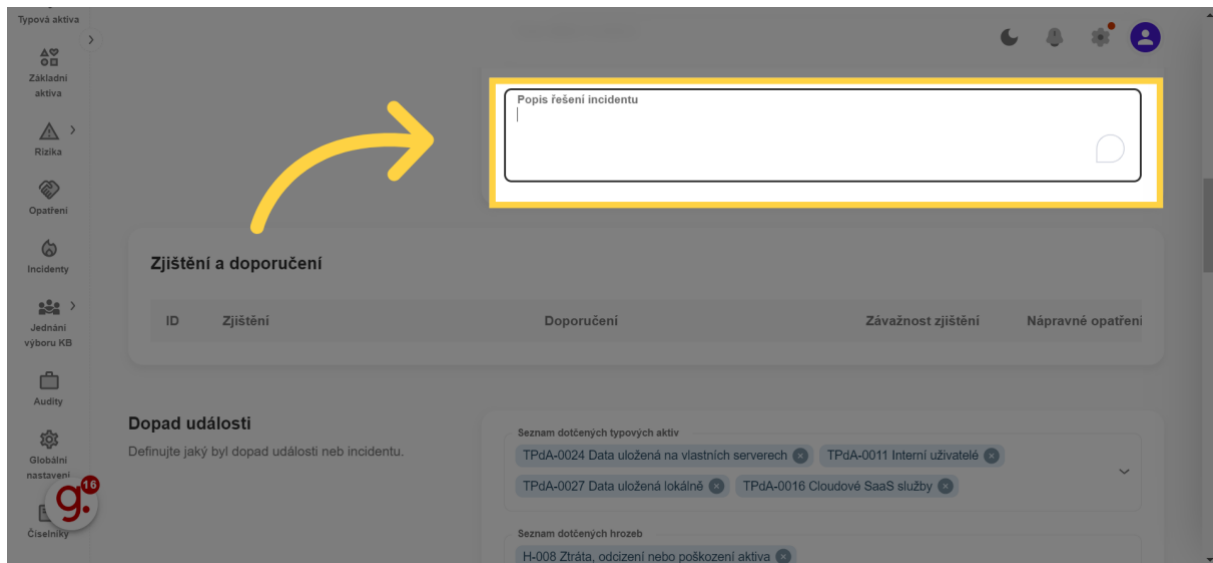
24. Číslo hlášení

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

The screenshot shows the MoyaKybeon interface. On the left is the same sidebar as in the previous image. The main area has a header 'Číslo hlášení incidentu' which is highlighted with a yellow box. A yellow arrow points from the left towards this field. Below this field is a section titled 'Zjištění a doporučení' with a table that has columns: 'ID', 'Zjištění', 'Doporučení', 'Závažnost zjištění', and 'Nápravné opatření'. Below the table is a section titled 'Dopad události' with the text 'Definujte jaký byl dopad události neb incidentu.' and a list of 'Seznam dotčených typových aktiv' including 'TPdA-0024 Data uložena na vlastních serverech', 'TPdA-0011 Interní uživatelé', 'TPdA-0027 Data uložena lokálně', and 'TPdA-0016 Cloudové SaaS služby'.

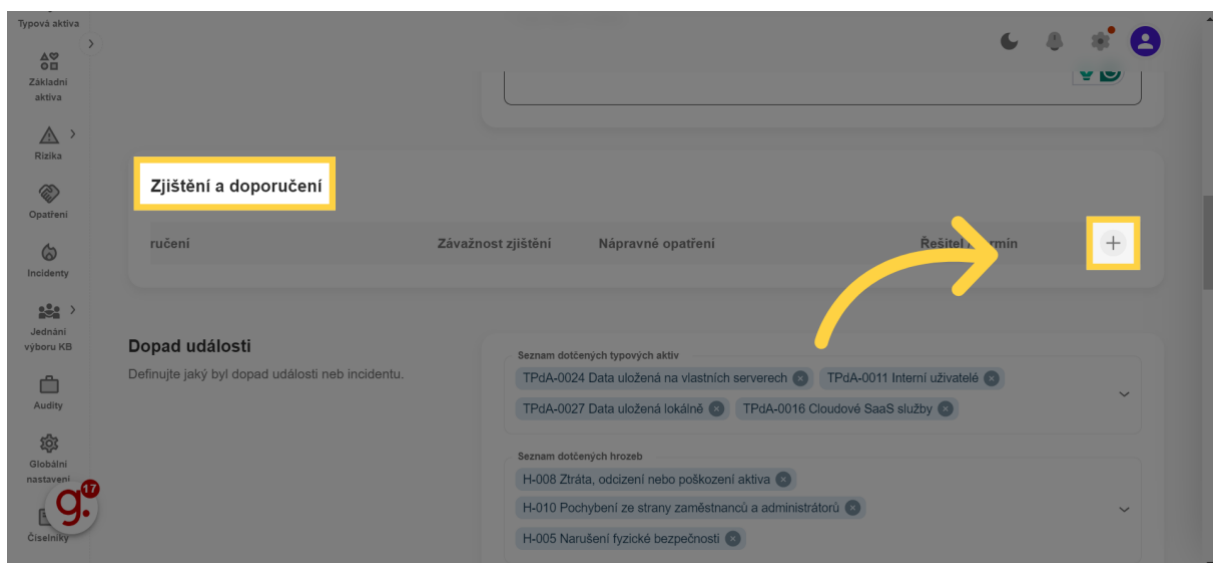
25. Popis řešení

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.

The screenshot shows the 'Zjištění a doporučení' section of the Moya Kybeon interface. The table has columns for ID, Zjištění, Doporučení, Závažnost zjištění, and Nápravné opatření. The first row (ID 1) has a yellow box around the 'Zjištění' input field, which contains the text 'Zjištění'. A yellow arrow points from the right towards this field. Below the table, there is a 'Dopad události' section and a 'Seznam dotčených typových aktiv' section.

28. Doporučení

A následně doplňte stručný popis doporučení.

The screenshot shows the 'Zjištění a doporučení' section of the Moya Kybeon interface. The table has columns for ID, Zjištění, Doporučení, Závažnost zjištění, and Nápravné opatření. The first row (ID 1) has a yellow box around the 'Doporučení' input field, which contains the text 'Doporučení'. A yellow arrow points from the left towards this field. Below the table, there is a 'Dopad události' section and a 'Seznam dotčených typových aktiv' section.

29. Závažnost

Pomocí plus a mínus nastavte závažnost zjištění.

The screenshot shows the 'Zjištění a doporučení' (Findings and Recommendations) section of the Moya Kybeon interface. A yellow arrow points from the 'Doporučení' (Recommendations) column to the 'Závažnost zjištění' (Severity of finding) column. The 'Závažnost zjištění' column contains a control with a minus sign, the number '0', and a plus sign. The 'Nápravné opatření' (Corrective action) column is also visible. The interface includes a sidebar with navigation icons and a top bar with user profile and settings icons.

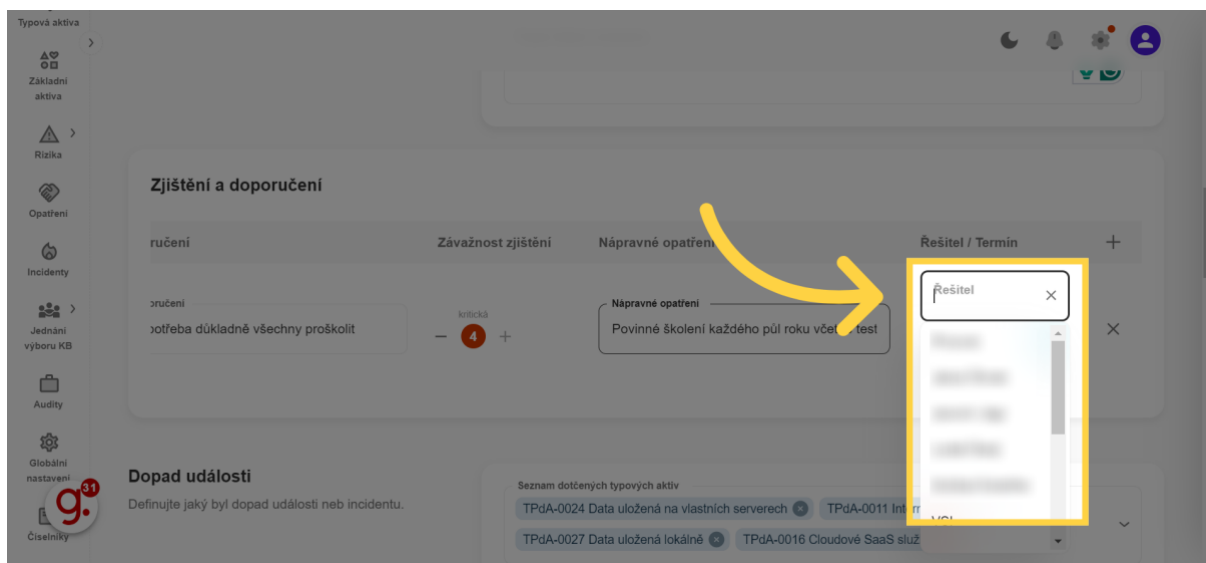
30. Nápravné opatření

Popište navrhované nápravné opatření.

The screenshot shows the 'Zjištění a doporučení' (Findings and Recommendations) section of the Moya Kybeon interface. A yellow arrow points from the 'Doporučení' (Recommendations) column to the 'Nápravné opatření' (Corrective action) column. The 'Nápravné opatření' column contains a text input field labeled 'Nápravné opatření'. The 'Závažnost zjištění' (Severity of finding) column is also visible. The interface includes a sidebar with navigation icons and a top bar with user profile and settings icons.

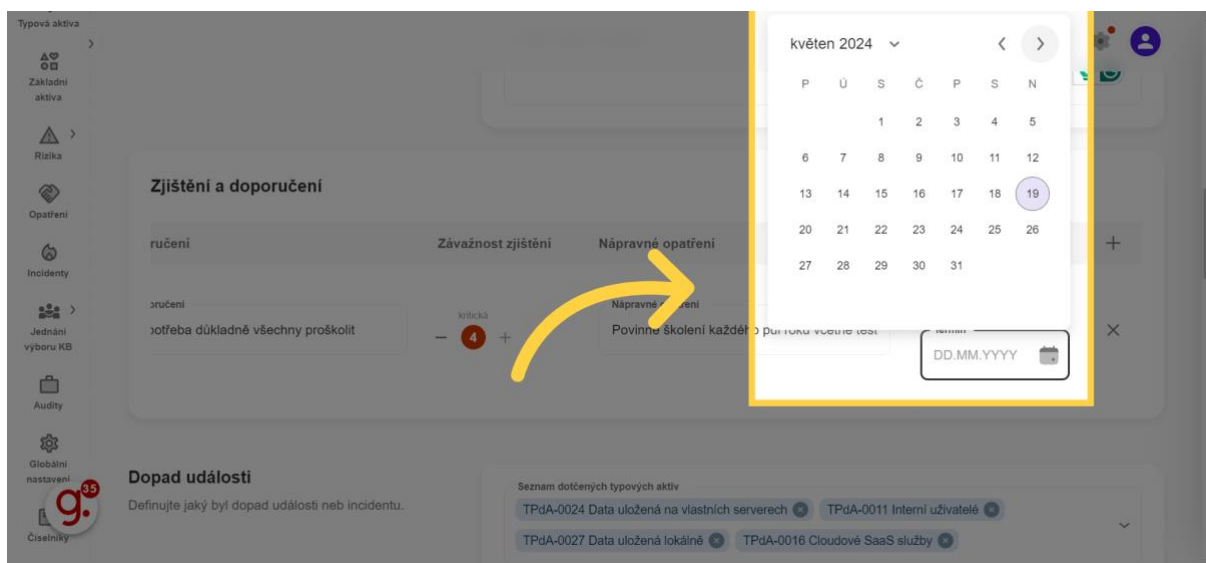
31. Řešitel

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.

Zjištění a doporučení

ID	Zjištění	Doporučení	Závažnost zjištění	Nápravné opatření	Řešení / Termin
1	Zjištění uživatelé stále nečtou	Doporučení proškolení všech uživatelů a prav	4	Nápravné opatření školení	Řešení Přidání opatření 30.11.2024 Nastavit automatické opatření
2	Zjištění Lorem ipsum dolor sit amet conso	Doporučení Lorem ipsum dolor sit amet conso	5	Nápravné opatření Lorem ipsum dolor sit amet conso	Řešení TEST KYBEON 1 25.09.2025 Uživatel je identifikován

34. Dopad události

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

Dopad události

Definujte, jaký byl dopad incidentu, nebo události.

Související rizika

Všechna rizika 2 Stávající rizika 2 Nová rizika 0

Související rizika

Typová aktivita	Hrozba	Zranitelnost
TPSA-0014 Administrátor - externí	TPSA-0022 Autonomní multifunkční školení zařízení	
TPSA-0025 Data uložena na zálohovacích médích	TPSA-0012 Externí uživatelé	
H-013 Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónských technik		
H-012 Dlouhodobá přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb		
Z-008 Nedostatečné monitorování činnosti lidských zdrojů, neschopnost odhalit jejich pochybení, nevhodná nebo závažná způsobů chování		

35. Dokončení

Kliknutím na Dokončit uzavřete zpracování incidentu v aplikaci MoyaKybeon.

