THE PROBLEM
WITH CYBERSECURITY
podla ChatGPT

what are the biggest problems in cybersecurity for SME's right now?

Here are some of the **biggest cybersecurity problems** facing small and medium-sized enterprises (SMEs) right now (2025) — plus notes on *why* they're issues and some pointers for mitigation. Since you're working with SMEs (albeit in accessories / e-commerce) this should help frame your thinking.

---

1. Limited resources + lack of specialised expertise

- Many SMEs simply don't have the budget or staff to build an in-house security team, monitor 24/7, or stay on top of evolving threats. SCIRP +2
- They may also lack awareness or cybersecurity literacy: what threats exist, how to detect, how to respond. arXiv
- Because of that, SMEs often are easier targets for attackers (less "hardening"). NCX Group
  Why it matters: If your business is digitally active (webshop, payment integration, cloud infrastructure) these limitations create gaps attackers can exploit.

Pointers: Prioritise core controls (patching, backups, strong passwords, multi-factor authentication), consider outsourcing to a managed service for security monitoring, allocate budget for regular training / awareness for your staff.

---

2. Phishing, social engineering & human error

- Phishing remains one of the top entry vectors for attackers targeting SMEs. Cyber Tech Guar... +2
- Human error (clicking malicious link, weak password, mis-configured cloud share) remains a big vulnerability. IT Pro +1
  Why it matters: Regardless of how good your technology is, if people are not trained or aware, attackers will exploit that "weak link".

Pointers: Run basic training with your team (even small team), phishing-simulations (if possible), enforce MFA for all key systems, adopt principle of least privilege (so a single error doesn't lead to full compromise).

---

3. Ransomware & extortion-type attacks

THE PROBLEM
WITH CYBERSECURITY
podla ChatGPT

5. Supply-chain, third-party & vendor risks

- SMEs may not only be targets themselves, they also may be weaker links in the supply chain of larger organisations. Attacks through third-party vendors or software dependencies are rising. securityexceptio... +1
  Why it matters: Even if your systems are relatively secure, if you integrate with or depend on other vendors/suppliers who are not, you may still get compromised via them.

Pointers: Evaluate your vendors: their security practices, what access they have to your systems/data. Limit vendor permissions to "just enough". Include security clauses in vendor contracts. Monitor vendor access.

---

6. Lack of incident-response preparedness & resilience

- Many SMEs do not have formal incident-response plans, lack testing of backup/restoration, or lack continuity planning. IT Pro +1
  Why it matters: If you *are* breached, your ability to respond, recover, restore operations will determine how much damage you suffer.

Pointers: Create a basic incident response plan (who does what when you detect a breach), perform tabletop exercises even informally, ensure you know how you'll communicate (internally + externally), know which backups you'll restore and how.

---

7. Evolving / sophisticated threats (AI-powered, targeted)

- Attackers are adopting more advanced tactics: AI-driven phishing, highly-targeted attacks, etc. WardenShield +1
  Why it matters: What used to be low-hanging fruit is evolving. If you assume "we're too small to be noticed", that's a dangerous mindset.

Pointers: Stay up to date with threat intelligence at least at a high level, ensure you have layers of defence (not just one security control), consider adopting "detect and respond" mindset not just "prevent".

---

8. Regulatory/compliance burdens & business risk awareness

- In many jurisdictions (especially EU) SMEs are increasingly subject to regulations (data protection, breach reporting, etc). Also cybersecurity is a **business risk** (not just an IT issue) — leadership awareness is still often lacking. The Times +1
  Why it matters: If you treat cybersecurity only as "IT's job", you may miss bigger business-impact issues: e.g., reputational damage, customer trust, supply-chain compliance, liability.

Pointers: Elevate cybersecurity to board/leadership level (even if small business) — ensure someone is

COMPLIANCE
CYBERSECURITY

Ako môže softvérová platforma s AI vylepšiť výkon manažérov kybernetickej bezpečnosti

Problém:

vyriešiť súlad s legislatívou a popri tom aj

reálne zlepšiť bezpečnosť.

Za rozumné náklady.

Legislatíva 1

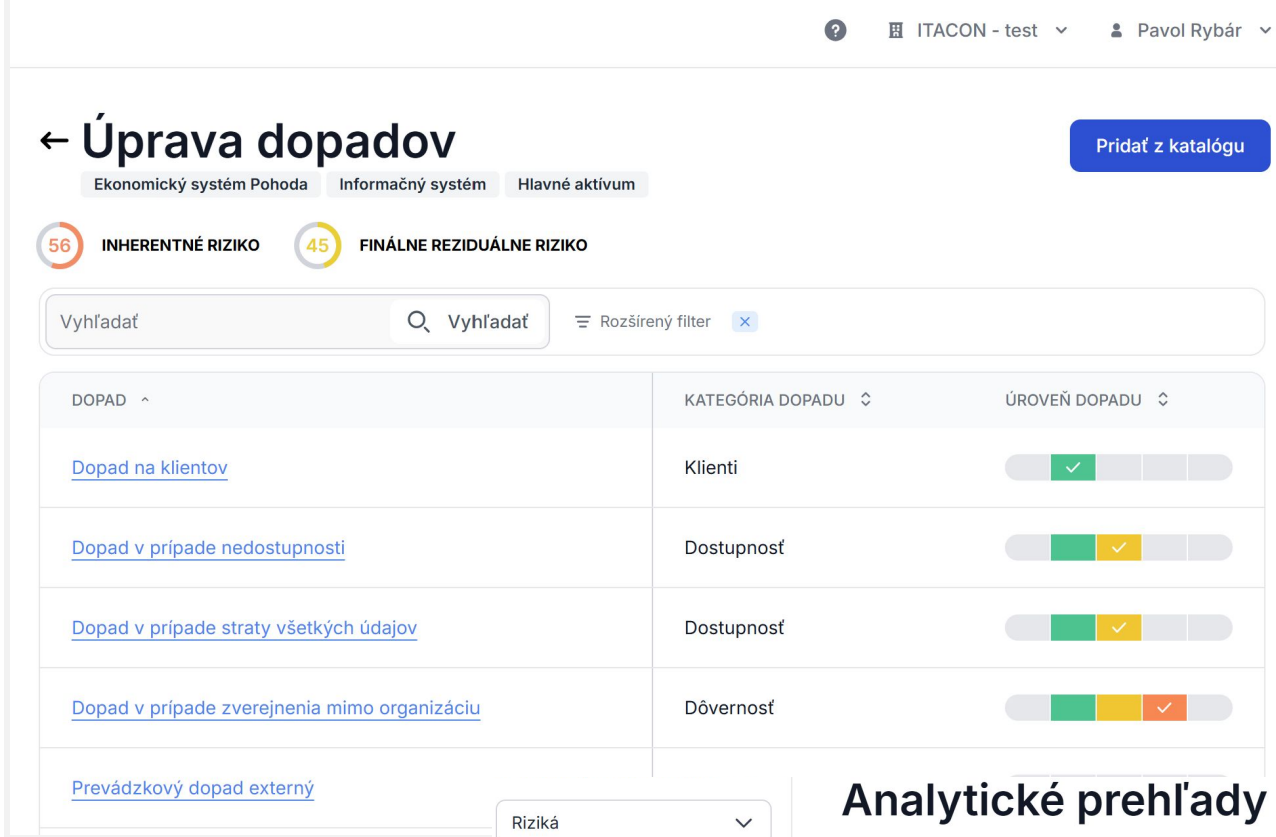
Zákon o KB / NIS2:

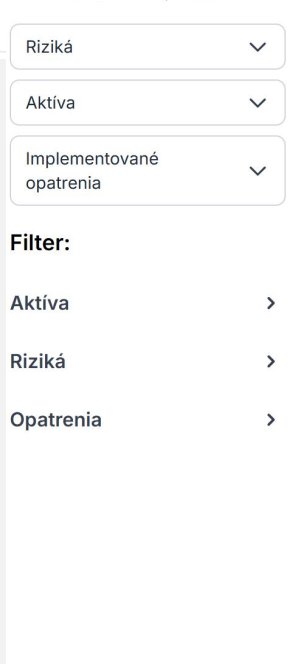
- analýza rizík
- tretie strany
- evidencia zmien
- evidencia incidentov
- BCM
- smernice
- všetko na jednom mieste

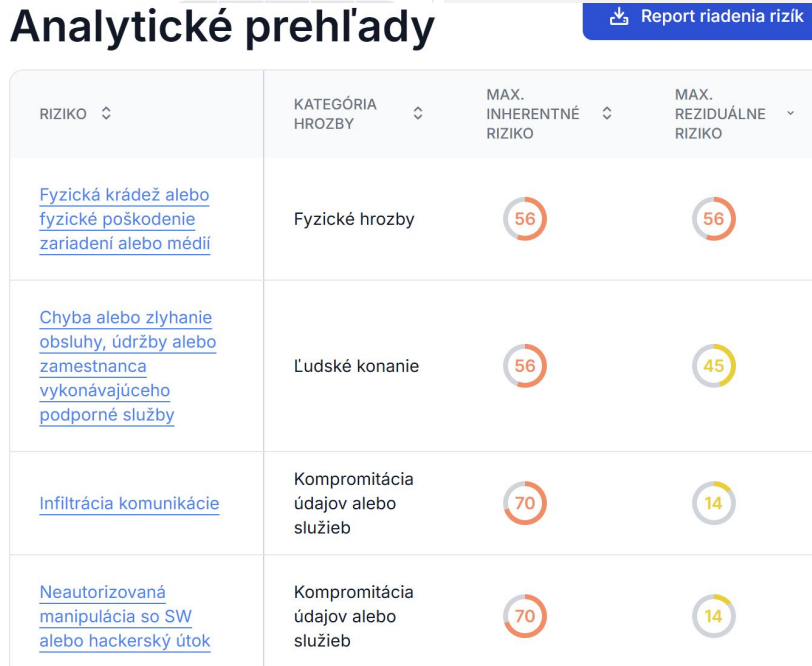
GDPR (roadmapa)

DORA (roadmapa)

Tazilla







Legislatíva 2

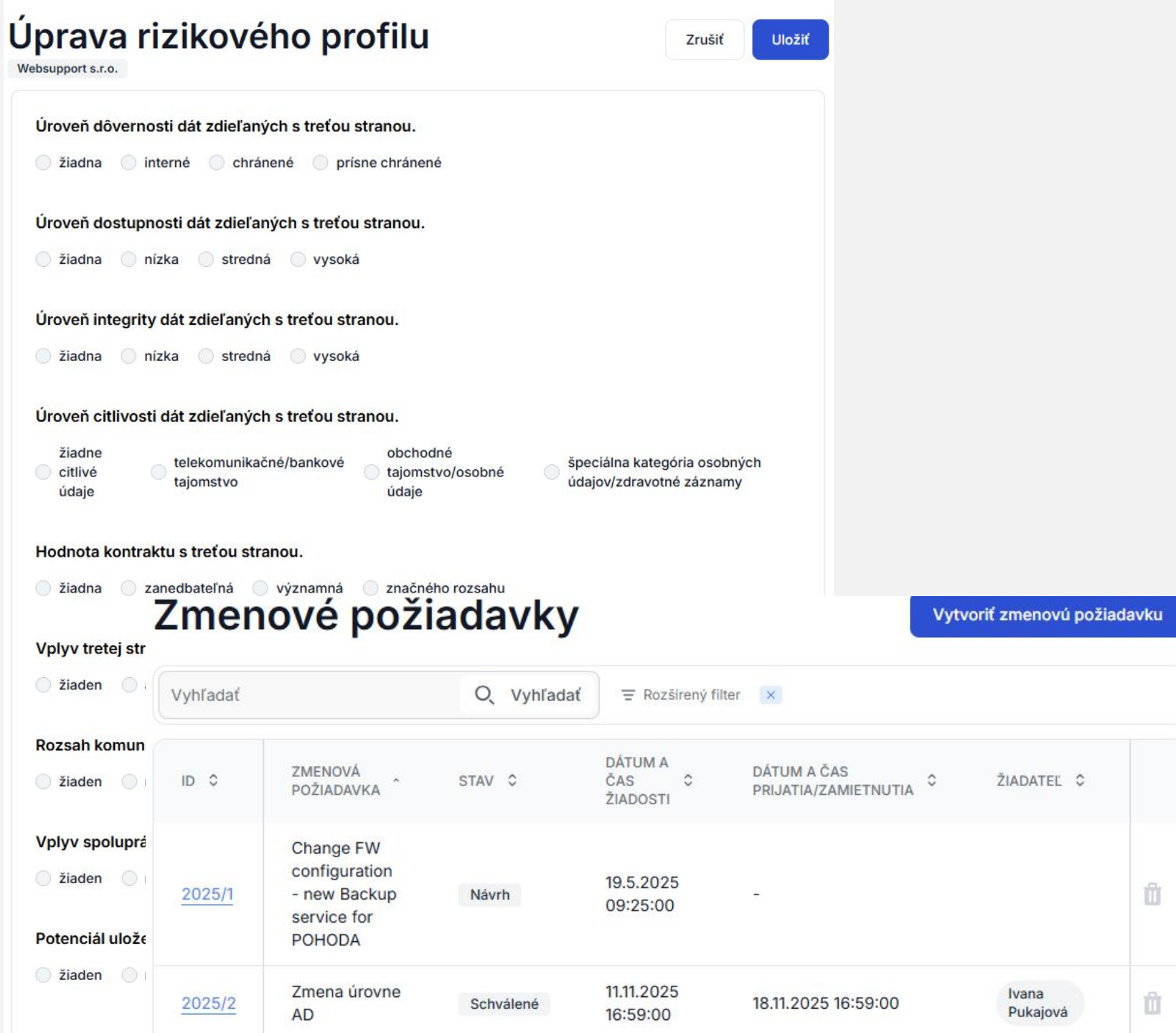
Zákon o KB / NIS2:

- analýza rizík
- tretie strany
- evidencia zmien
- evidencia incidentov
- BCM
- smernice
- všetko na jednom mieste

GDPR (roadmapa)

DORA (roadmapa)

Tazilla



Legislatíva 3

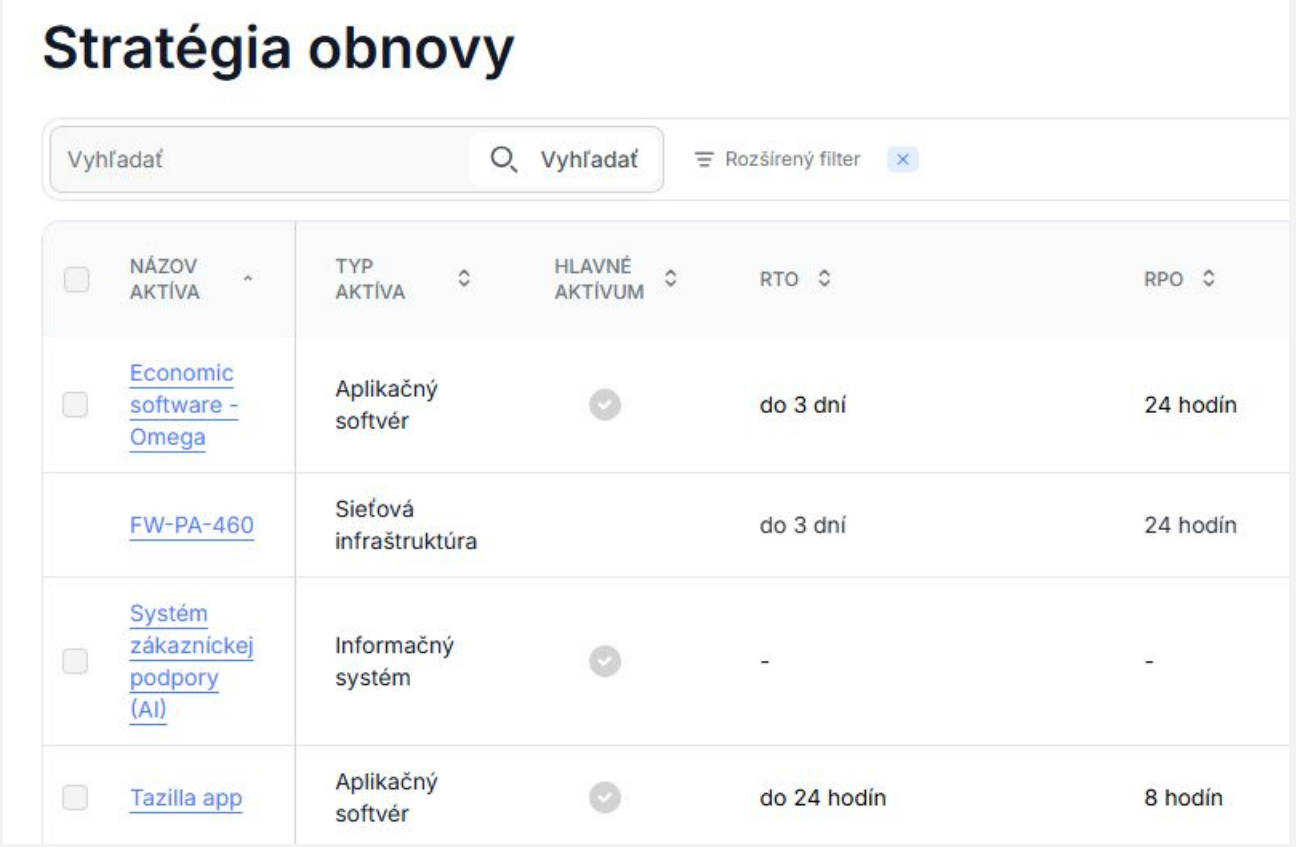
Zákon o KB / NIS2:

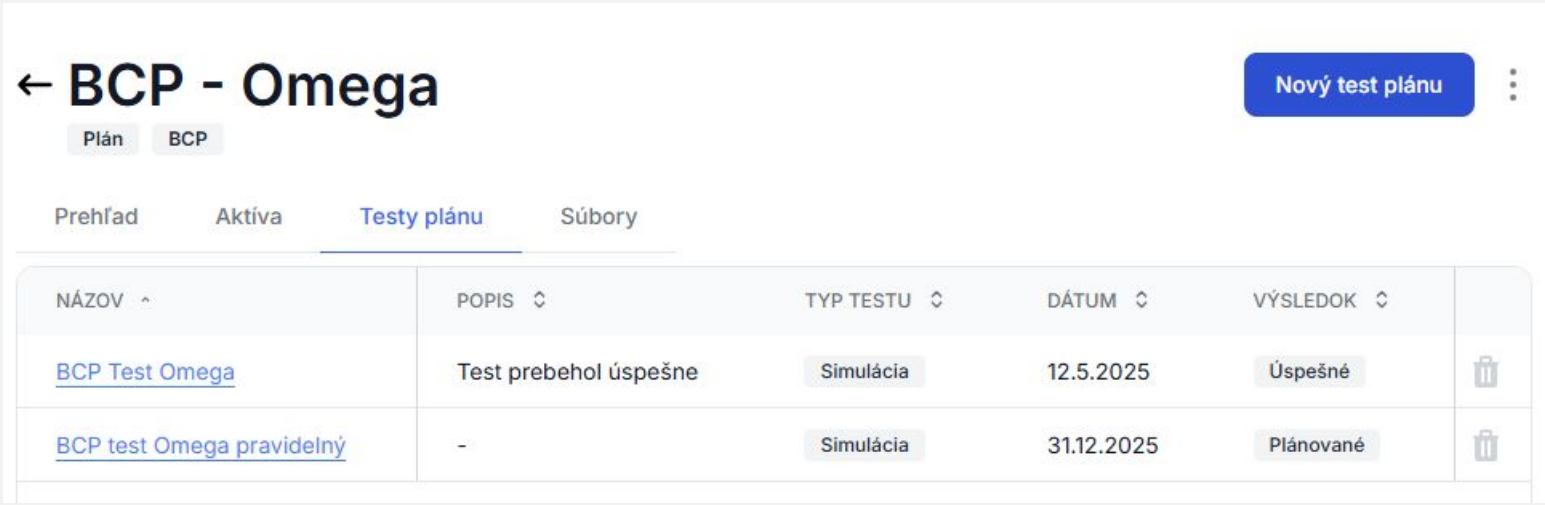
- analýza rizík
- tretie strany
- evidencia zmien
- evidencia incidentov
- BCM
- smernice
- všetko na jednom mieste

GDPR (roadmapa)

DORA (roadmapa)

Tazilla





Legislatíva 4

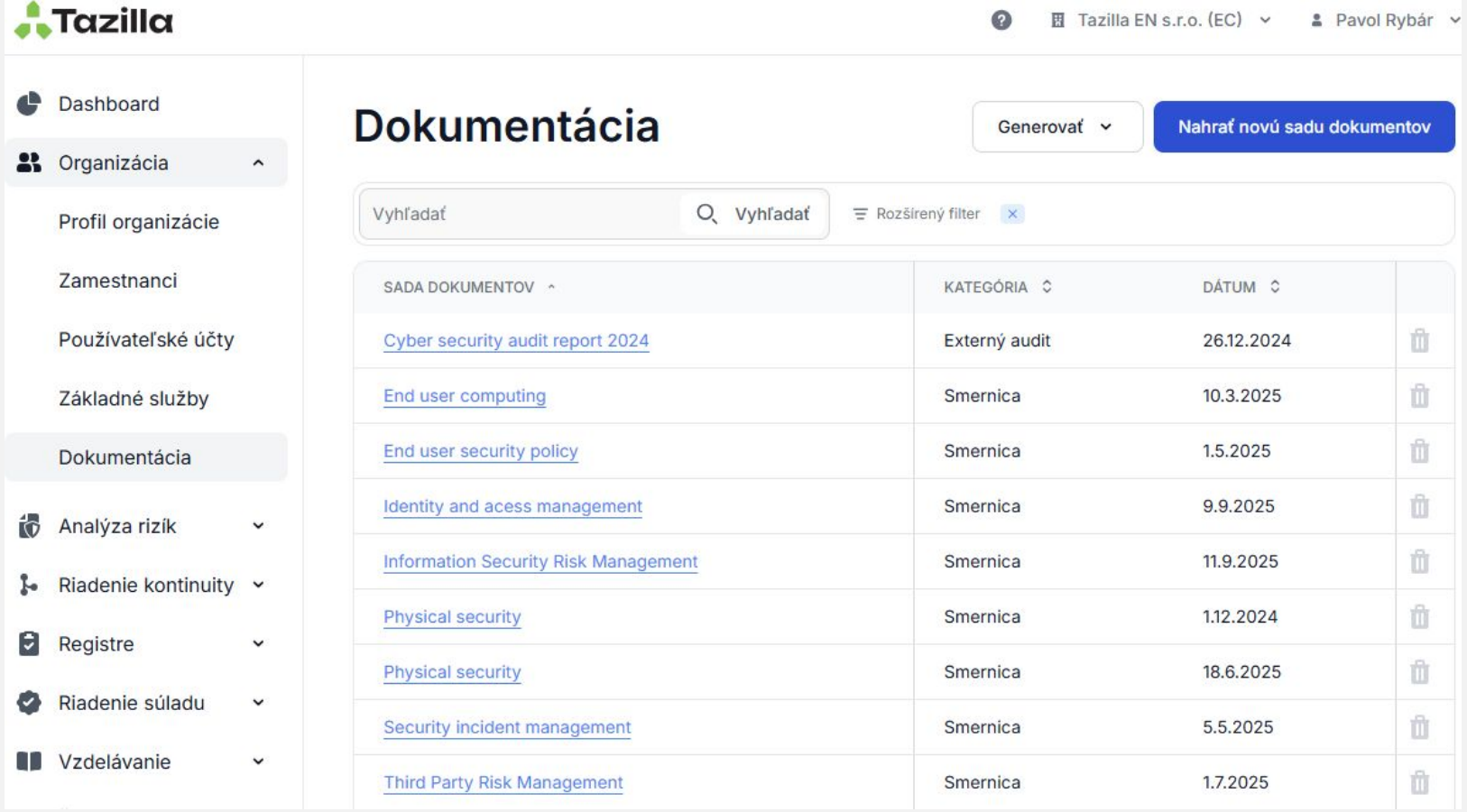
Zákon o KB / NIS2:

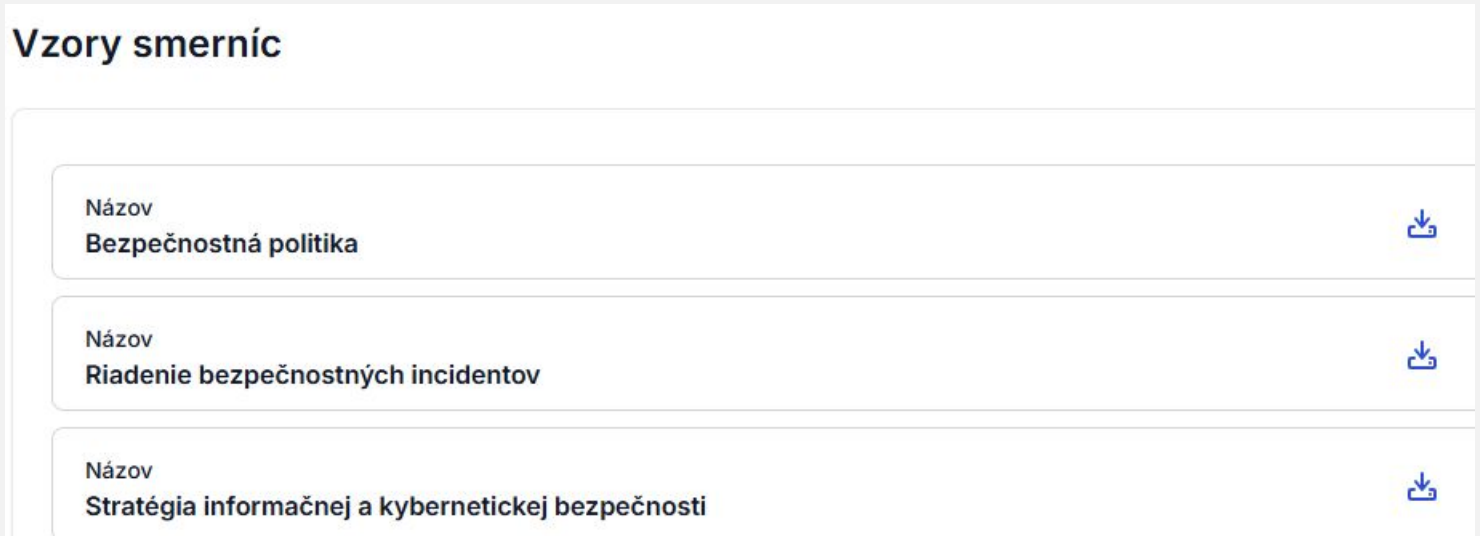
- analýza rizík
- tretie strany
- evidencia zmien
- evidencia incidentov
- BCM
- smernice
- všetko na jednom mieste

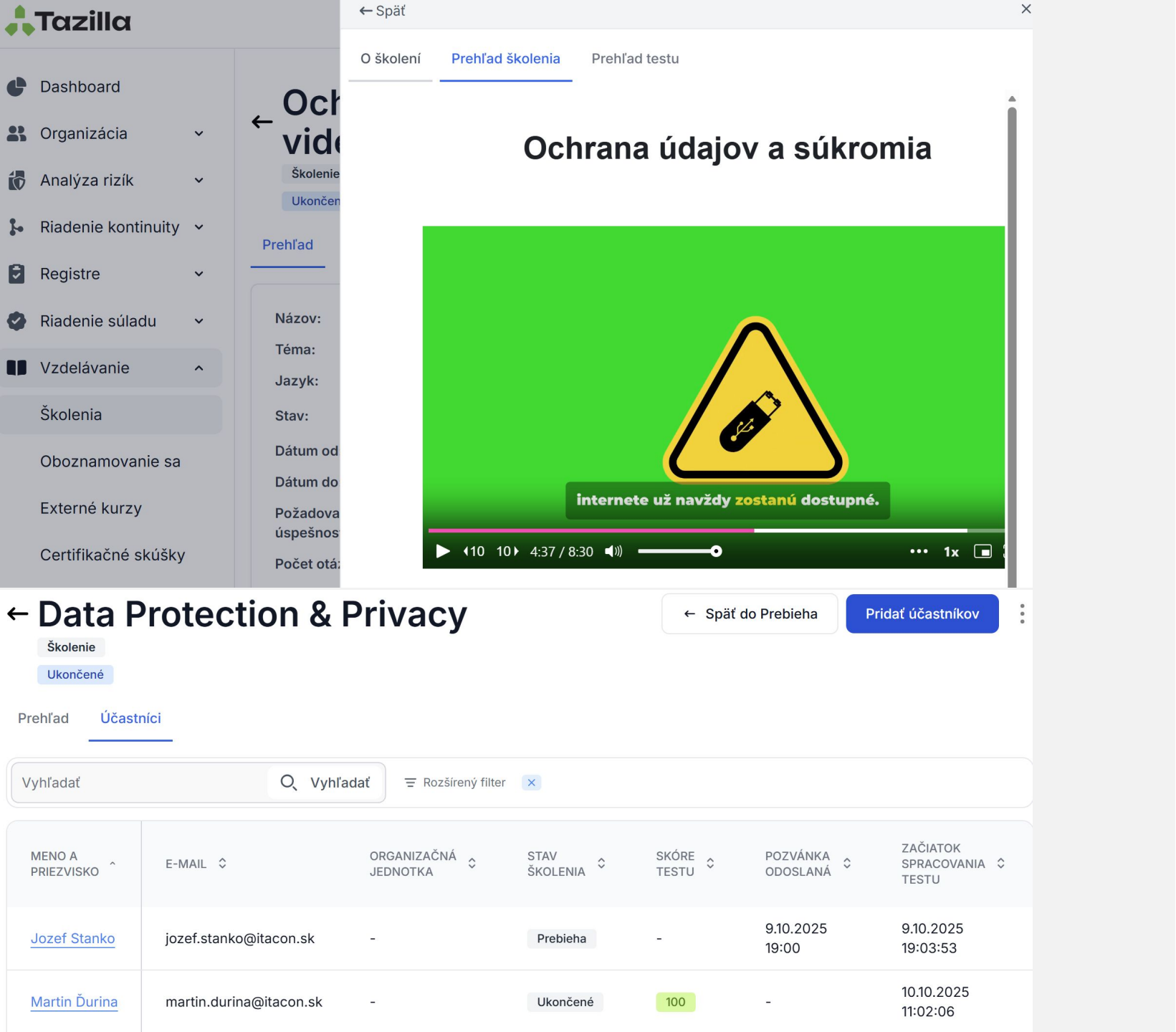
GDPR (roadmapa)

DORA (roadmapa)

Tazilla







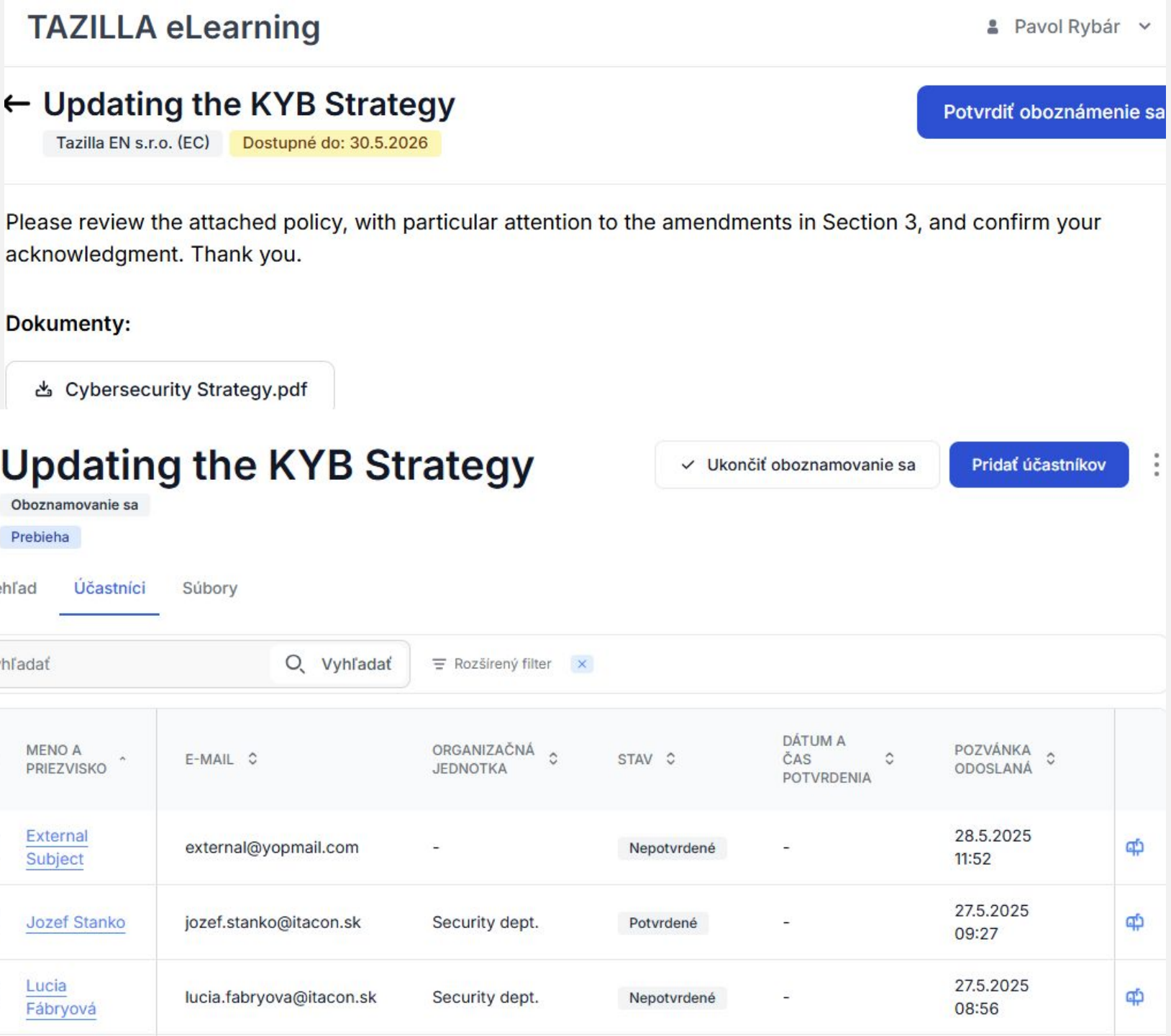
Reálna bezpečnosť: vzdelávanie 1

Plán vzdelávania

Školenia zamestnancov

Oboznamovanie sa

Tazilla



Reálna bezpečnosť: vzdelávanie 2

Plán vzdelávania

Školenia zamestnancov

Oboznamovanie sa

Tazilla

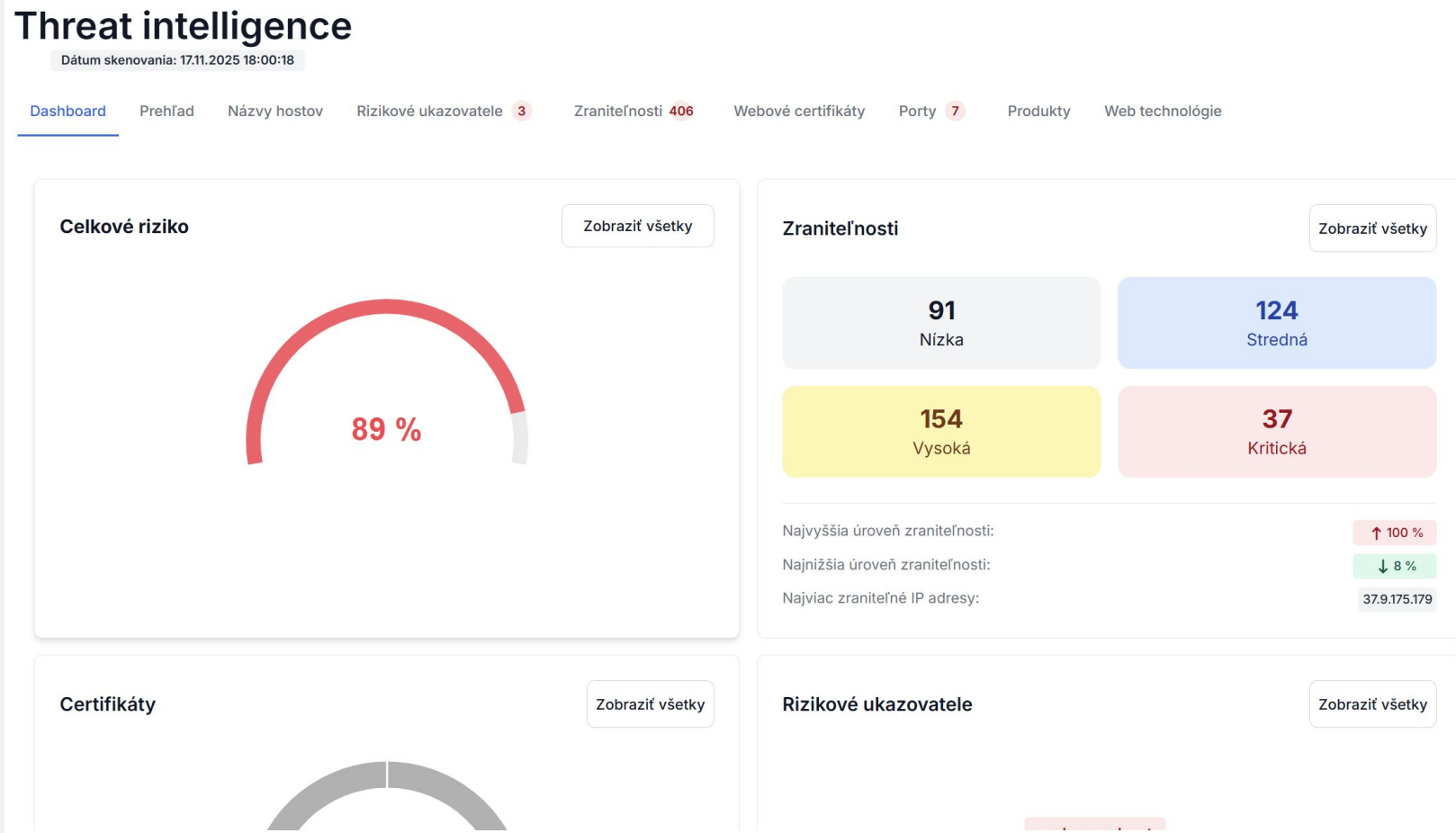
Reálna bezpečnosť: zraniteľnosti 1

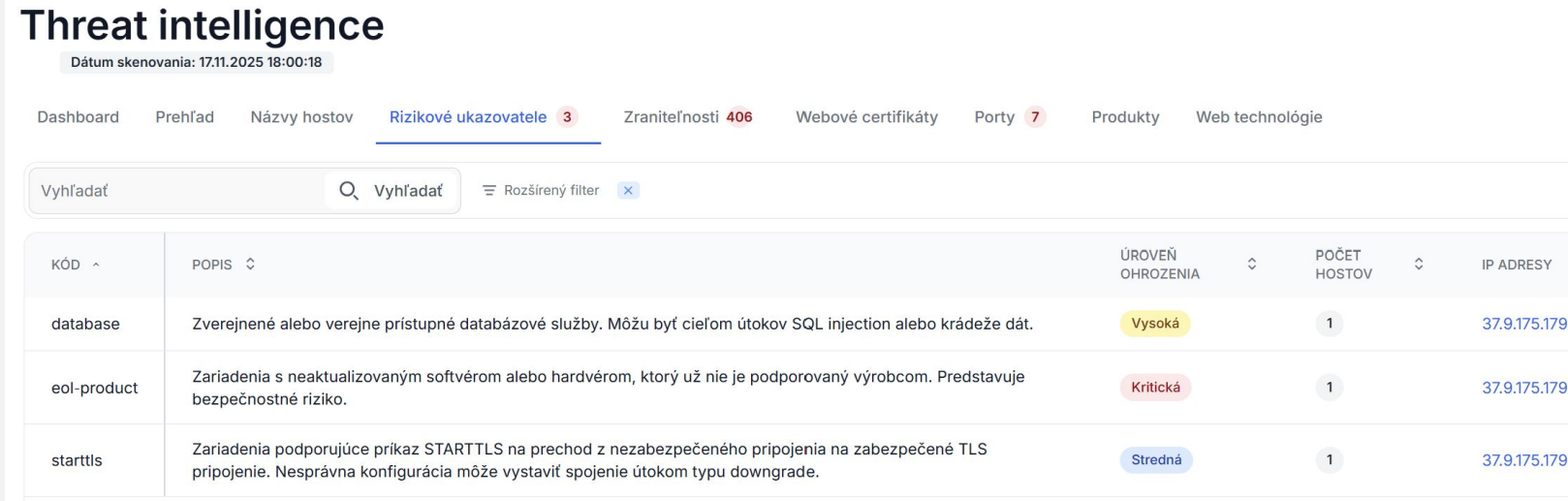
Threat intel

Skenovanie zraniteľností

Analýza kódu

Tazilla



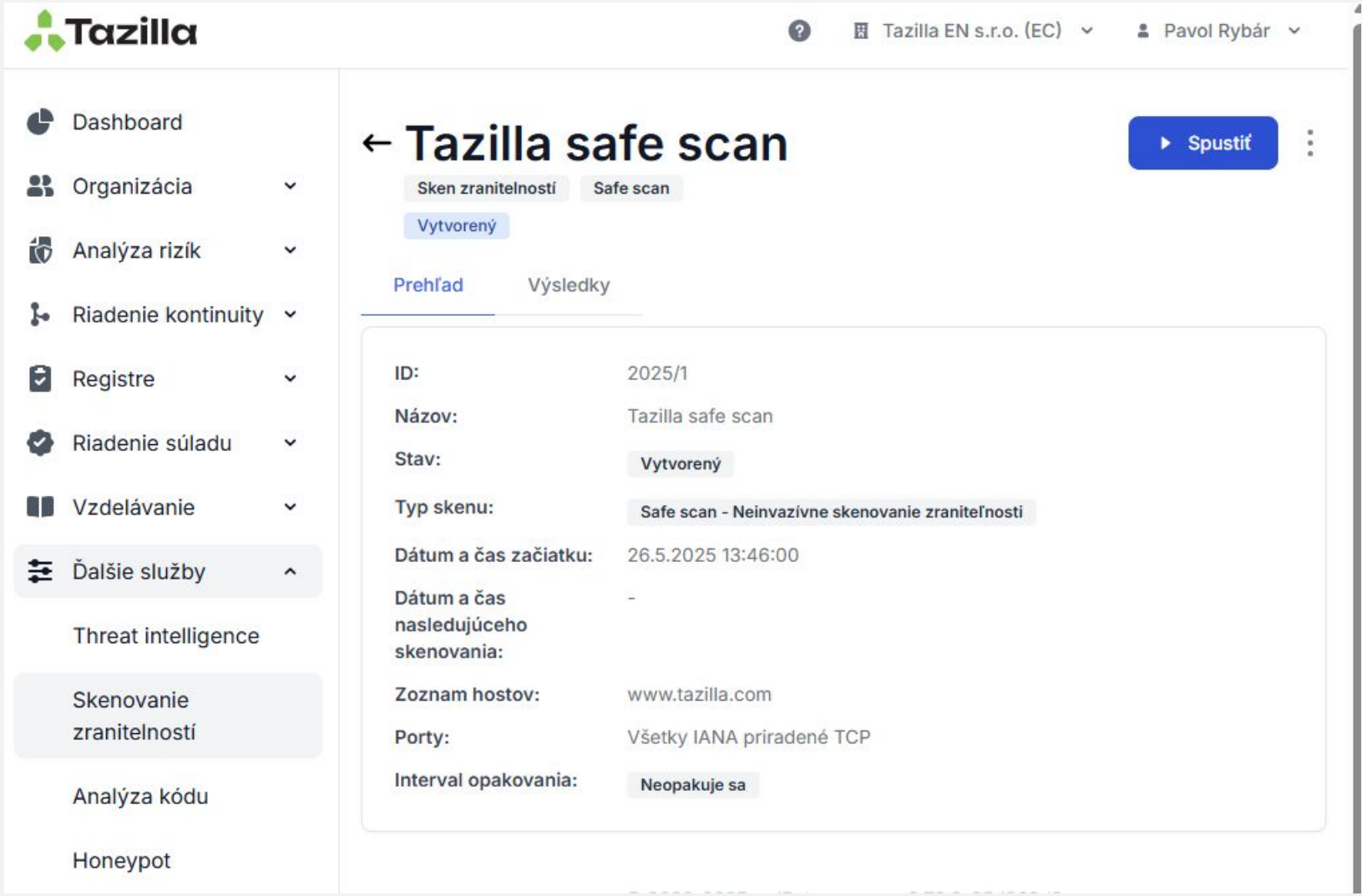


Reálna bezpečnosť: zraniteľnosti 2

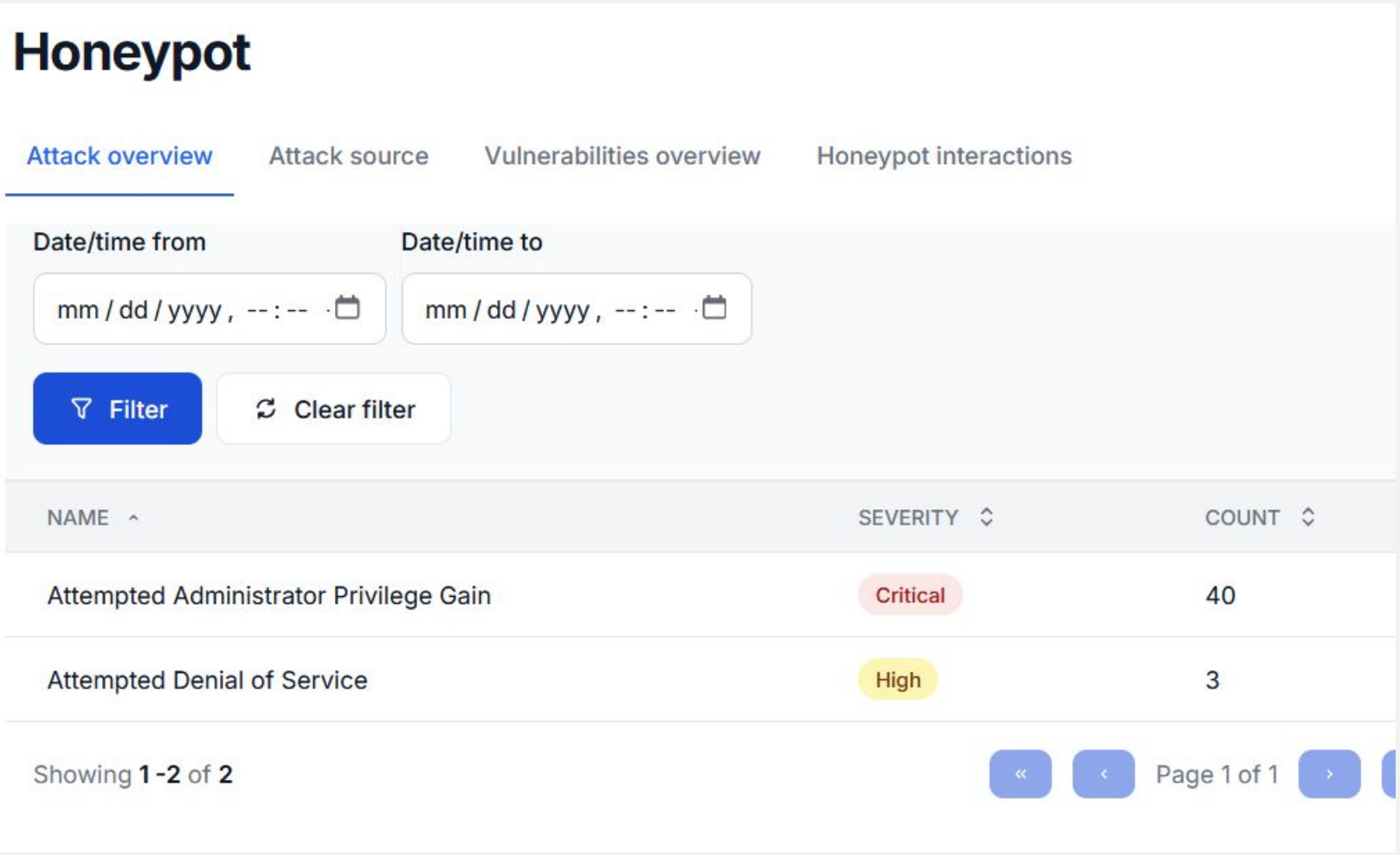
Threat intel

Skenovanie zraniteľností

Analýza kódu



Tazilla



Reálna bezpečnosť: prevencia a detekcia

Honeypot

Phishing test

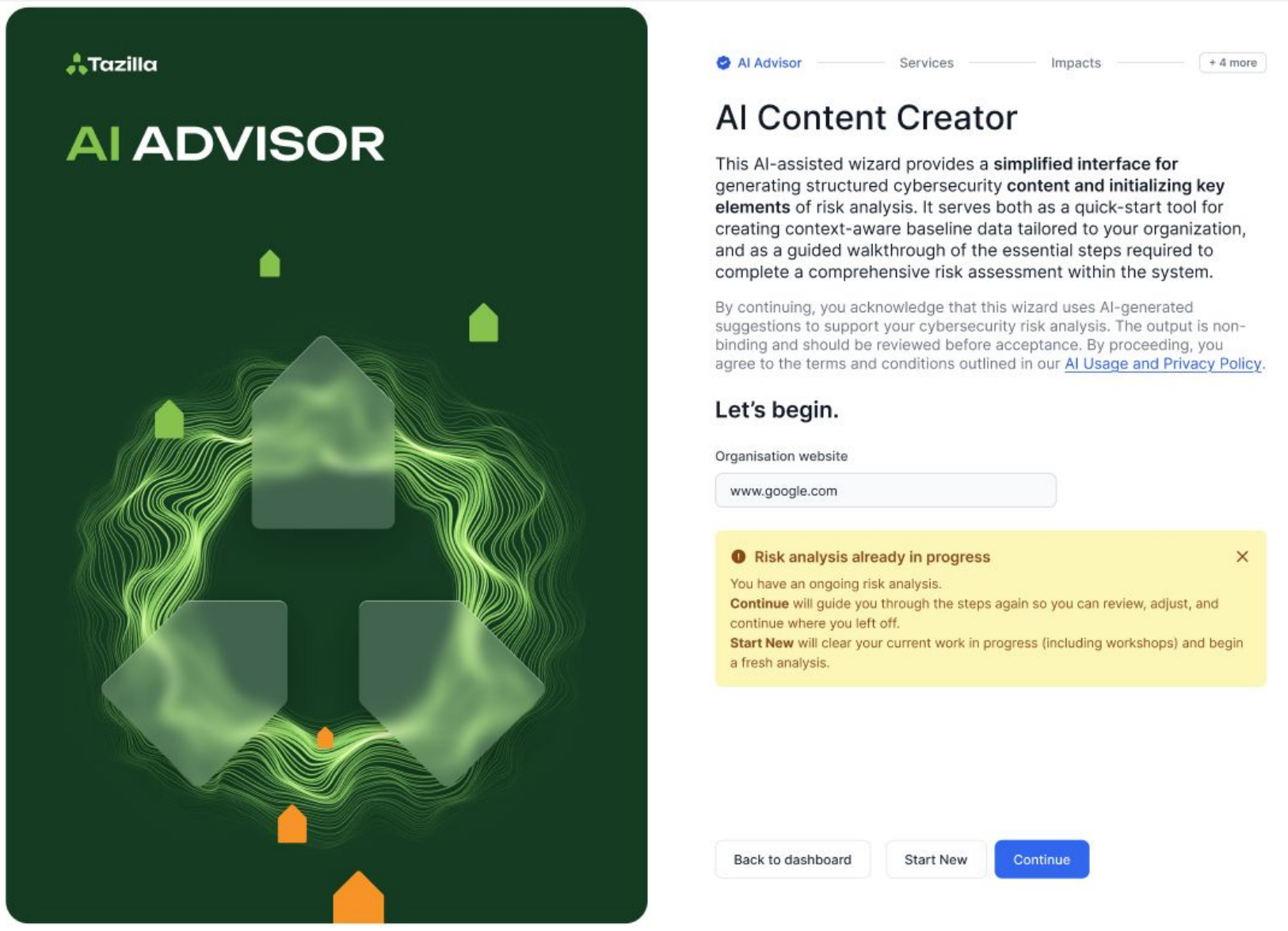
Tazilla

AI onboarding

AI zistí voľne dostupné údaje z internetu

Vyplní prázdny profil

Ušetrí čas používateľovi



Tazilla

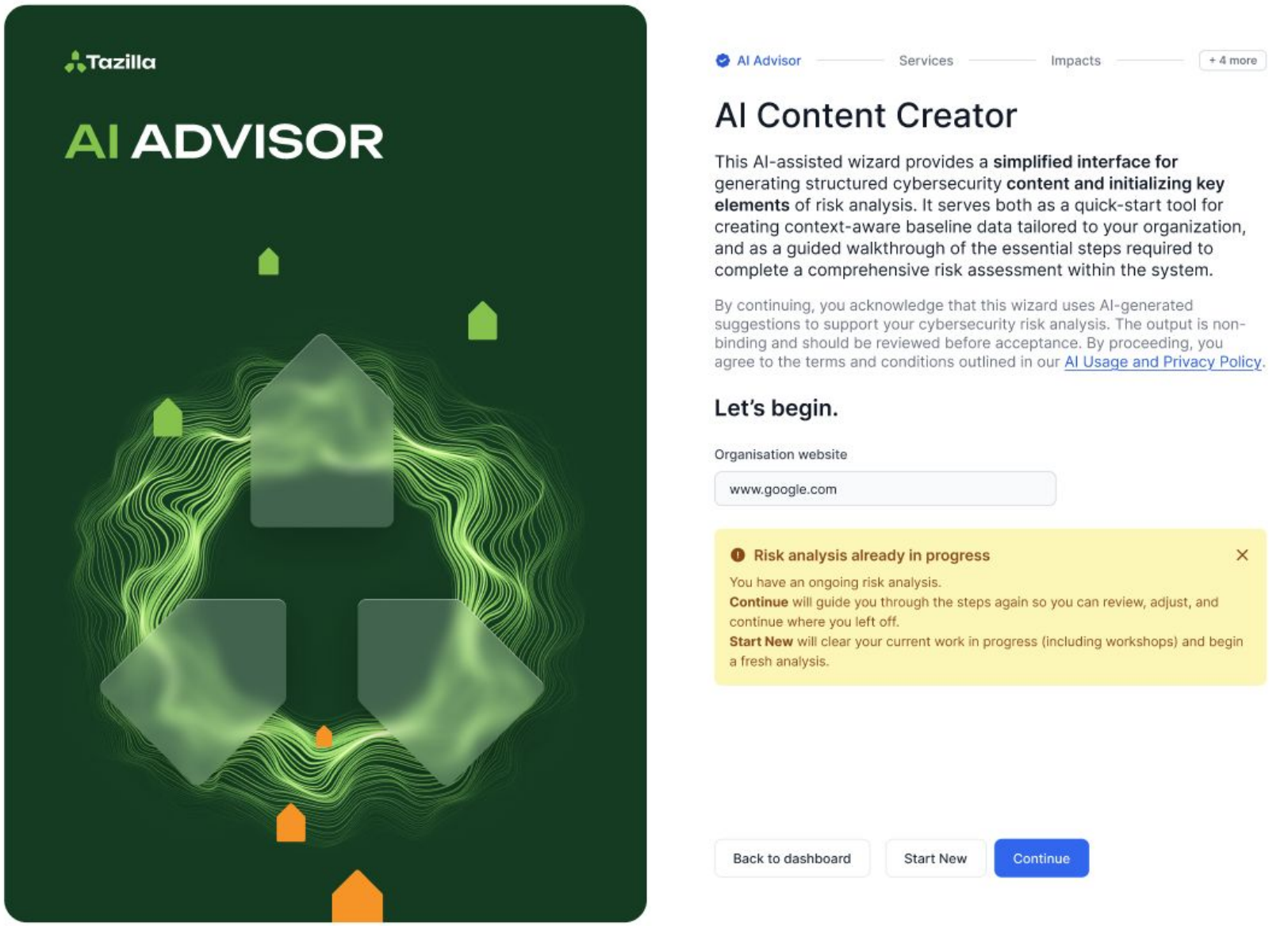
AI
analýza rizík

Analýza rizík „je rocket science“

Tazilla

AI
analýza rizík

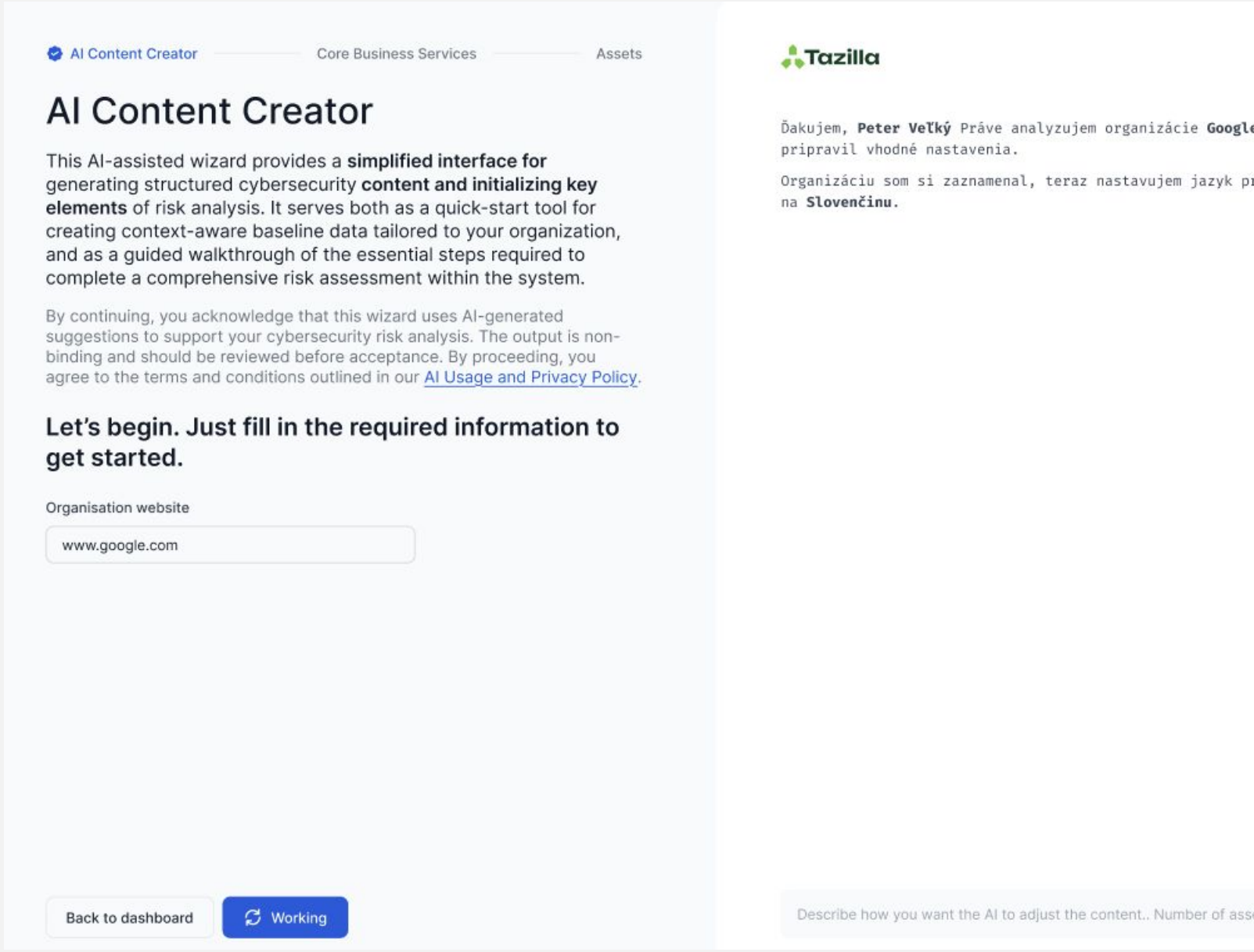
Preto ju s AI spravíme na mieru pomocou verejných info



Tazilla

AI analýza rizík

Preto ju s AI spravíme na mieru pomocou verejných info



Tazilla

what are the biggest problems in cybersecurity for SME's right now?

Here are some of the **biggest cybersecurity problems** facing small and medium-sized enterprises (SMEs) right now (2025) — plus notes on *why* they're issues and some pointers for mitigation. Since you're working with SMEs (albeit in accessories / e-commerce) this should help frame your thinking.

---

1. Limited resources + lack of specialised expertise

- Many SMEs simply don't have the budget or staff to build an in-house security team, monitor 24/7, or stay on top of evolving threats. SCIRP +2
- They may also lack awareness or cybersecurity literacy: what threats exist, how to detect, how to respond. arXiv
- Because of that, SMEs often are easier targets for attackers (less "hardening"). NCX Group
  Why it matters: If your business is digitally active (webshop, payment integration, cloud infrastructure) these limitations create gaps attackers can exploit.

Pointers: Prioritise core controls (patching, backups, strong passwords, multi-factor authentication), consider outsourcing to a managed service for security monitoring, allocate budget for regular training / awareness for your staff.

---

2. Phishing, social engineering & human error

- Phishing remains one of the top entry vectors for attackers targeting SMEs. Cyber Tech Guar... +2
- Human error (clicking malicious link, weak password, mis-configured cloud share) remains a big vulnerability. IT Pro +1
  Why it matters: Regardless of how good your technology is, if people are not trained or aware, attackers will exploit that "weak link".

Pointers: Run basic training with your team (even small team), phishing-simulations (if possible), enforce MFA for all key systems, adopt principle of least privilege (so a single error doesn't lead to full compromise).

---

3. Ransomware & extortion-type attacks

5. Supply-chain, third-party & vendor risks

- SMEs may not only be targets themselves, they also may be weaker links in the supply chain of larger organisations. Attacks through third-party vendors or software dependencies are rising. securityexceptio... +1
  Why it matters: Even if your systems are relatively secure, if you integrate with or depend on other vendors/suppliers who are not, you may still get compromised via them.

Pointers: Evaluate your vendors: their security practices, what access they have to your systems/data. Limit vendor permissions to "just enough". Include security clauses in vendor contracts. Monitor vendor access.

---

6. Lack of incident-response preparedness & resilience

- Many SMEs do not have formal incident-response plans, lack testing of backup/restoration, or lack continuity planning. IT Pro +1
  Why it matters: If you *are* breached, your ability to respond, recover, restore operations will determine how much damage you suffer.

Pointers: Create a basic incident response plan (who does what when you detect a breach), perform tabletop exercises even informally, ensure you know how you'll communicate (internally + externally), know which backups you'll restore and how.

---

7. Evolving / sophisticated threats (AI-powered, targeted)

- Attackers are adopting more advanced tactics: AI-driven phishing, highly-targeted attacks, etc. WardenShield +1
  Why it matters: What used to be low-hanging fruit is evolving. If you assume "we're too small to be noticed", that's a dangerous mindset.

Pointers: Stay up to date with threat intelligence at least at a high level, ensure you have layers of defence (not just one security control), consider adopting "detect and respond" mindset not just "prevent".

---

8. Regulatory/compliance burdens & business risk awareness

- In many jurisdictions (especially EU) SMEs are increasingly subject to regulations (data protection, breach reporting, etc). Also cybersecurity is a **business risk** (not just an IT issue) — leadership awareness is still often lacking. The Times +1
  Why it matters: If you treat cybersecurity only as "IT's job", you may miss bigger business-impact issues: e.g., reputational damage, customer trust, supply-chain compliance, liability.

Pointers: Elevate cybersecurity to board/leadership level (even if small business) — ensure someone is accountable; consider including it in your risk-register; keep abreast of regulatory obligations (breach notification, minimum security controls, etc).

Financovaný Európskou úniou

www.tazilla.com

Beta verzia zdarma do 04/2026

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE