
Proces Threat Intelligence (Threat Intelligence Process)

Verze: 1.1

Platnost od: 27. 01. 2026

Garant procesu: Security Officer / IT Administrátor

Vazba na ISO/IEC 27001:2022:

- A.5.7 – Threat Intelligence
- A.8.8 – Správa technických zranitelností

---

1. Účel

Účelem tohoto procesu je systematický sběr, analýza a využití informací o kybernetických hrozbách a zranitelnostech relevantních pro telemetrický ekosystém organizace. Proces umožňuje včasnou identifikaci rizik, jejich prioritizaci a provázání s technickými a procesními opatřeními.

2. Rozsah

Proces se vztahuje na:

- backendovou infrastrukturu,
- CI/CD pipeline a použité knihovny,
- telemetrické jednotky a firmware,
- síťovou a bezpečnostní infrastrukturu (EDR, FW, API).

3. Zdroje informací o hrozbách

Organizace využívá kombinaci následujících zdrojů:

- **Veřejné databáze zranitelností:** CVE, NVD (National Vulnerability Database).
- **Bezpečnostní bulletiny dodavatelů:** Cloud platformy, CI/CD nástroje, knihovny třetích stran, výrobci HW/SIM/modemů.
- **Národní a sektorové autority:** NÚKIB, CSIRT.cz, CERT-EU (pokud relevantní).
- **Interní bezpečnostní data:** Logy z EDR, aplikačních firewallů, CI/CD security nástrojů (SAST/SCA).

4. Životní cyklus Threat Intelligence

Proces probíhá jako kontinuální cyklus:

1. **Sběr (Collection):** Pravidelná kontrola zdrojů (min. týdně, u kritických alertů okamžitě).
2. **Analýza relevance (Analysis):** Posouzení dopadu na používaná aktiva (např. knihovny v CI/CD, FW komponenty, OS, cloud služby).
3. **Prioritizace (Prioritization):** Klasifikace dle CVSS a kontextu: **Critical** (≥ 9.0), **High**, **Medium**, **Low**.
4. **Reakce (Action):** Návrh opatření (patch/update, změna konfigurace, dočasná mitigace, eskalace do Change Managementu).
5. **Distribuce (Dissemination):** Předání výstupů odpovědným rolím (IT, Vývoj, Management).

5. Reakce na kritické hrozby (0-day)

Při identifikaci kritické zranitelnosti s dostupným exploitem:

- **Aktivace nouzového režimu:** Security Officer zahajuje incidentový nebo krizový postup.
- **Časový rámec:** Zahájení mitigace nebo nápravného opatření do 24 hodin.
- **Vazba na změny:** Použije se režim Emergency Change dle *Politiky řízení změn*.
- **Dokumentace:** Veškeré kroky jsou evidovány pro audit a post-mortem analýzu.

6. Vazba na další procesy

Threat Intelligence je přímo provázána s:

- **Procesem správy technických zranitelností (A.8.8)**.
- **Secure CI/CD pipeline** (blokace buildů při kritických CVE).
- **Change Managementem** (standardní vs. nouzové změny).
- **Incident Response** (pokud hrozba přeroste v incident).

7. Odpovědnosti

- **Security Officer:** Sleduje zdroje hrozeb, vyhodnocuje relevanci a prioritu, eskaluje kritické hrozby.
- **IT Administrátor:** Provádí patching a konfigurační změny, ověřuje účinnost mitigací.
- **Lead Developer:** Řeší zranitelnosti v kódu a závislostech, aktualizuje knihovny v CI/CD pipeline.

8. Auditní důkazy

Organizace uchovává:

- TI reporty (měsíční přehled hrozeb a jejich dopadu).
- Vazbu CVE → opatření (patch, změna, mitigace).
- Výstupy vulnerability scanů potvrzující odstranění rizik.
- Záznamy emergency změn u kritických hrozeb.