# 12 Konverze záznamů kybernetických incidentů

Excel@FIT 2019

**Autor:**
**Pavel Eis**

**Vedoucí práce:**
**Ing. Martin Žádník, Ph.D.**

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

## Motivace

Cílem této práce je navrhnout způsob **konverze mezi formáty určené pro uchování záznamů o kybernetických incidentech**. Konvertovanými formáty jsou formát **IDEA** využívaný sdružením **Cesnet**, formát sdílecí platformy **MISP** a proprietární verze formátu **STIX** platformy **C3ISP**. Při konverzi je důležité dbát na postup, aby nedošlo ke ztrátě důležitých informací, nebo aby při chybném převodu nevznikl jiný druh události, než byl ten původní.

## Výsledky

**Výstupem** této práce jsou:

- **2 konvertory** (konverzní knihovny) - první provádí konverzi mezi formáty IDEA a MISP a druhý provádí konverzi mezi formáty IDEA a STIX
- **4 konektory** - každý obsluhuje jeden směr konverze

Vzniklé konvertory a konektory umožňují sdílet kybernetické incidenty mezi organizacemi, které je mohou využít k hlubší a širší analýze aktuálních hrozeb.

Základní vlastnosti konvertovaných formátů (zelené podbarvení řádku značí stejné vlastnosti, oranžové podbarvení řádku značí pouze podobné vlastnosti).

| IDEA | MISP | STIX (C3ISP) |
|---|---|---|
| Informace o bezpečnostních událostech a incidentech | Informace z různých domén (bezpečnostní incidenty, analýza malware, blacklisty IP adres, ...) | Informace o bezpečnostních událostech a incidentech |
| Popis incidentu pomocí síťových informací (IP, MAC, port, protokol ...) | Popis incidentu pomocí síťových informací (IP, MAC, port, protokol ...) | Popis incidentu pomocí síťových informací (IP, MAC, port, protokol ...) |
| Druh události: kategorie/taxonomie | Druh události: kategorie/taxonomie | Druh události: kategorie/taxonomie, textový popis |
| Jednotný styl informací | Jednotný styl informací | Několik schémat událostí, některé se sémanticky částečně odlišují |

### MISP

```
{
   "date": "2018-12-03",
   ...
   "Object": [
      {
         "name": "network-source",
         ...
         "Attribute": [
            {
               "category": "Payload delivery",
               "type": "ip-dst|port",
               "value": "192.168.0.1|5678",
               ...
            }, ...
         ]
      }
   ],
   "Tag": [
      {
         "name": "ecsirt:malicious-code=Trojan",
         ...
      },
      {
         "name": "rsit:malicious-code=Trojan",
         ...
      }
   ]
}
```

### STIX

```
{
   "type": "observed-data",
   "created": "2018-12-03T10:20:54Z,
   "cybox": {
      "objects": [
         "…|Ransom.Wannacry|low|cat=Trojan
         rt=2018-12-03T10:15:13Z
         dst=192.168.0.1 dpt=5678 ...",
         ...
      ]
   }
}
```

### IDEA

```
{
   "DetectTime": "2018-12-03T10:15:13Z",
   "CreateTime": "2018-12-03T10:20:54Z",
   "Category": ["Malware.Trojan"]
   ...
   "Target": [
      {
         "IP4": ["192.168.0.1"],
         "Port": [5678],
         ...
      }
   ],
   ...
}
```