PREDIKCIA BEZPEČNOSTNÝCH UDALOSTÍ POUŽITÍM VIACROZMERNÝCH MODELOV ČASOVÝCH RADOV

ŠTUDENT:	BC. MIROSLAV VOJTEK
VEDÚCI PRÁCE:	RNDR. JUDR. PAVOL SOKOL, PHD.
KONZULTANT:	RNDR. ANDREJ GAJDOŠ, PHD.

ÚVOD

- Časový rad – hodnoty, ktoré sú zhromažďované, zaznamenávané alebo pozorované postupne v čase
- Hlavný cieľ – predikcia bezpečnostných udalostí

DÁTA

- Záznamy o bezpečnostných udalostiach
  - pôvod – CESNET (idea.cesnet.cz)
  - viac ako 1 miliarda záznamov
- Záznamy o zraniteľnostiach
  - cve.mitre.org
  - nvd.nist.gov/vuln

```
{
   "Format": "IDEA0",
   "ID": "4390fc3f-c753-4a3e-bc83-1b44f24baf75",
   "CreateTime": "2012-11-03T10:00:02Z",
   "DetectTime": "2012-11-03T10:00:07Z",
   "WinStartTime": "2012-11-03T05:00:00Z",
   "WinEndTime": "2012-11-03T10:00:00Z",
   "EventTime": "2012-11-03T07:36:00Z",
   "CeaseTime": "2012-11-03T09:55:22Z",
   "Category": ["Fraud.Phishing"],
   "Ref": ["cve:CVE-1234-5678"],
   "Confidence": 1,
   "Note": "Synthetic example",
   "ConnCount": 20,
   "Source": [
      {
         "Type": ["Phishing"],
         "IP4": ["192.168.0.2-192.168.0.5", "192.168.0.10/25"],
         "IP6": ["2001:0db8:0000:0000:0000:ff00:0042::/112"],
         "Hostname": ["example.com"],
         "URL": ["http://example.com/cgi-bin/killemall"],
         "Proto": ["tcp", "http"],
         "AttachHand": ["att1"],
         "Netname": ["ripe:IANA-CBLK-RESERVED1"]
      }
   ],
```

```
"Source": [
    {
        "Type": ["Phishing"],
        "IP4": ["192.168.0.2-192.168.0.5", "192.168.0.10/25"],
        "IP6": ["2001:0db8:0000:0000:0000:ff00:0042::/112"],
        "Hostname": ["example.com"],
        "URL": ["http://example.com/cgi-bin/killemall"],
        "Proto": ["tcp", "http"],
        "AttachHand": ["att1"],
        "Netname": ["ripe:IANA-CBLK-RESERVED1"]
    }
],
"Target": [
    {
        "Type": ["Backscatter", "OriginSpam"],
        "Email": ["innocent@example.com"],
        "Spoofed": true
    },
    {
        "IP4": ["10.2.2.0/24"],
        "Anonymised": true
    }
],
```

```
    "Attach": [
        {
            "Handle": "att1",
            "FileName": ["killemall"],
            "Type": ["Malware"],
            "ContentType": "application/octet-stream",
            "Hash": ["sha1:0c4a38c3569f0cc632e74f4c"],
            "Size": 46,
            "Ref": ["Trojan-Spy:W32/FinSpy.A"],
            "ContentEncoding": "base64",
            "Content": "TVpqdXN0a2lkZGluZwo="
        }
    ],
    "Node": [
        {
            "Name": "cz.cesnet.kippo-honey",
            "Type": ["Protocol", "Honeypot"],
            "SW": ["Kippo"],
            "AggrWin": "00:05:00"
        }
    ]
}
```

CIELE PRÁCE

- Analyzovať možnosti použitia viacrozmerných modelov časových radov v kybernetickej bezpečnosti
- Preskúmať a porovnať metódy viacrozmerných modelov časových radov z pohľadu predikcie bezpečnostných udalostí
- Navrhnúť, implementovať a vyhodnotiť systém na predikciu bezpečnostných udalostí

NAJBLIŽŠIE KROKY

- Oboznámenie sa s aktuálnym stavom v tejto oblasti
- Zoznámenie sa s dátami
- Vytvorenie časových radov (udalosti a zraniteľnosti)
  - Udalosti – kategória, protokol, cieľový port, služba, ...
  - Zraniteľnosti – skóre, dopad, ...
- Naštudovanie vhodných metód

ŠTUDIJNÁ LITERATÚRA

- BOX, George EP, et al. Time series analysis: forecasting and control. John Wiley & Sons, 2015.
- ESLING, Philippe; AGON, Carlos. Time-series data mining. ACM Computing Surveys (CSUR), 2012, 45.1: 12.
- DUA, Sumeet; DU, Xian. Data mining and machine learning in cybersecurity. CRC press, 2016.

ĎAKUJEM ZA POZORNOSŤ

☺