PREDIKCIA BEZPEČNOSTNÝCH UDALOSTÍ POUŽITÍM VIACROZMERNÝCH MODELOV ČASOVÝCH RADOV

AUTOR: BC. MIROSLAV VOJTEK

VEDÚCI PRÁCE: RNDR. JUDR. PAVOL SOKOL, PHD.

KONZULTANT: RNDR. ANDREJ GAJDOŠ, PHD.

ČASOVÉ RADY

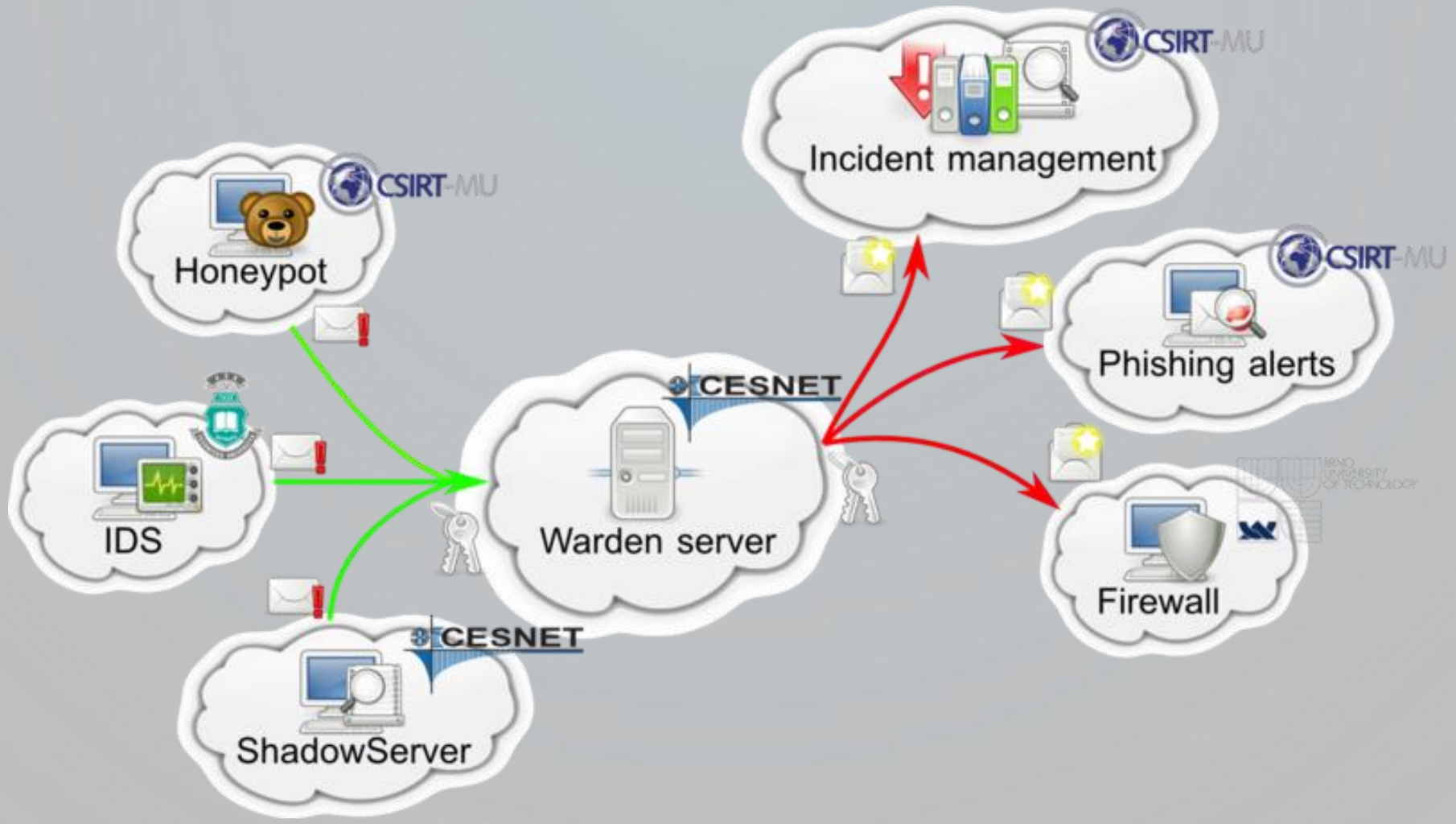
- **Časový rad** môžeme chápať ako zoznam zaznamenaných číselných hodnôt, pri ktorých máme informáciu, kedy boli zaznamenané
- Hodnoty môžu, ale aj nemusia byť zaznamenávané v pravidelných časových intervaloch

DÁTA - UDALOSTI

Bezpečnostné udalosti - záznamy

- pôvod – WARDEN, CESNET (idea.cesnet.cz)
- viac ako 1 miliarda záznamov
- 1 záznam = 1 alert v IDEA formáte
- časový úsek – cca 2 roky

WARDEN



https://warden.cesnet.cz/cs/architecture

```
{
    "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"]
        }
    ],
```


https://idea.cesnet.cz

```
"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
    }
],
```


https://idea.cesnet.cz

```
    "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"
        }
    ]
}
```


https://idea.cesnet.cz

DÁTA - UDALOSTI

Bezpečnostné udalosti – časové rady

- časová jednotka – 10, 30 a 60 minút
- kategória (recon scanning, ddos, attempt login, malware ransomware, ...)
- port (21, 22, 53, 80, 443, 445, ...)
- protokol (FTP, SSH, DNS, HTTP, ICMP, TCP, SSH, ...)
- ...

DÁTA – ZRANITEĽNOSTI

Záznamy o zraniteľnostiach

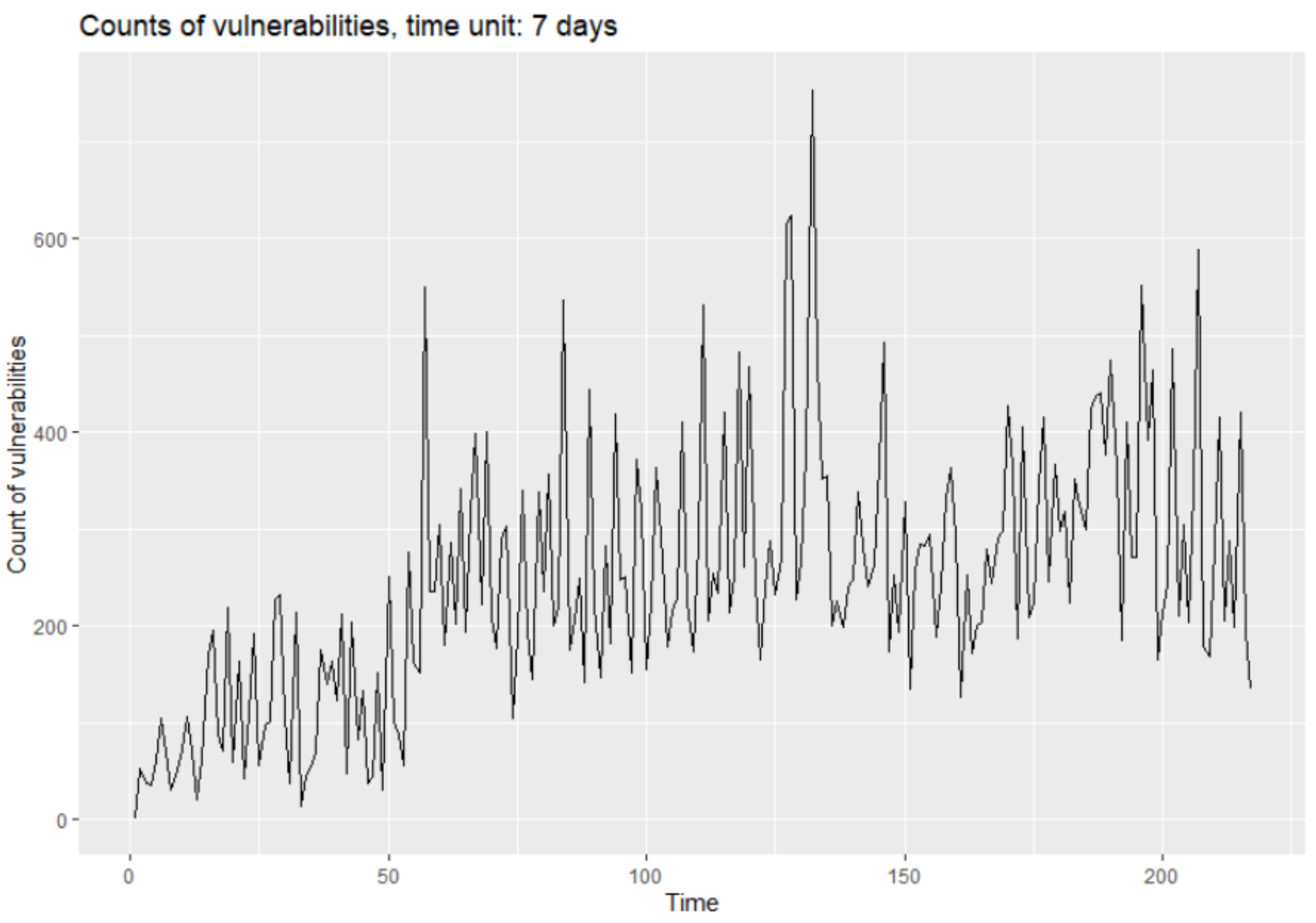
- cve.mitre.org (Common Vulnerabilities and Exposures)
- nvd.nist.gov/vuln (National Vulnerability Database)

DÁTA – ZRANITEĽNOSTI

CVSS (Common Vulnerability Scoring System)

- Základné metriky
- Časové
- Metriky prostredia

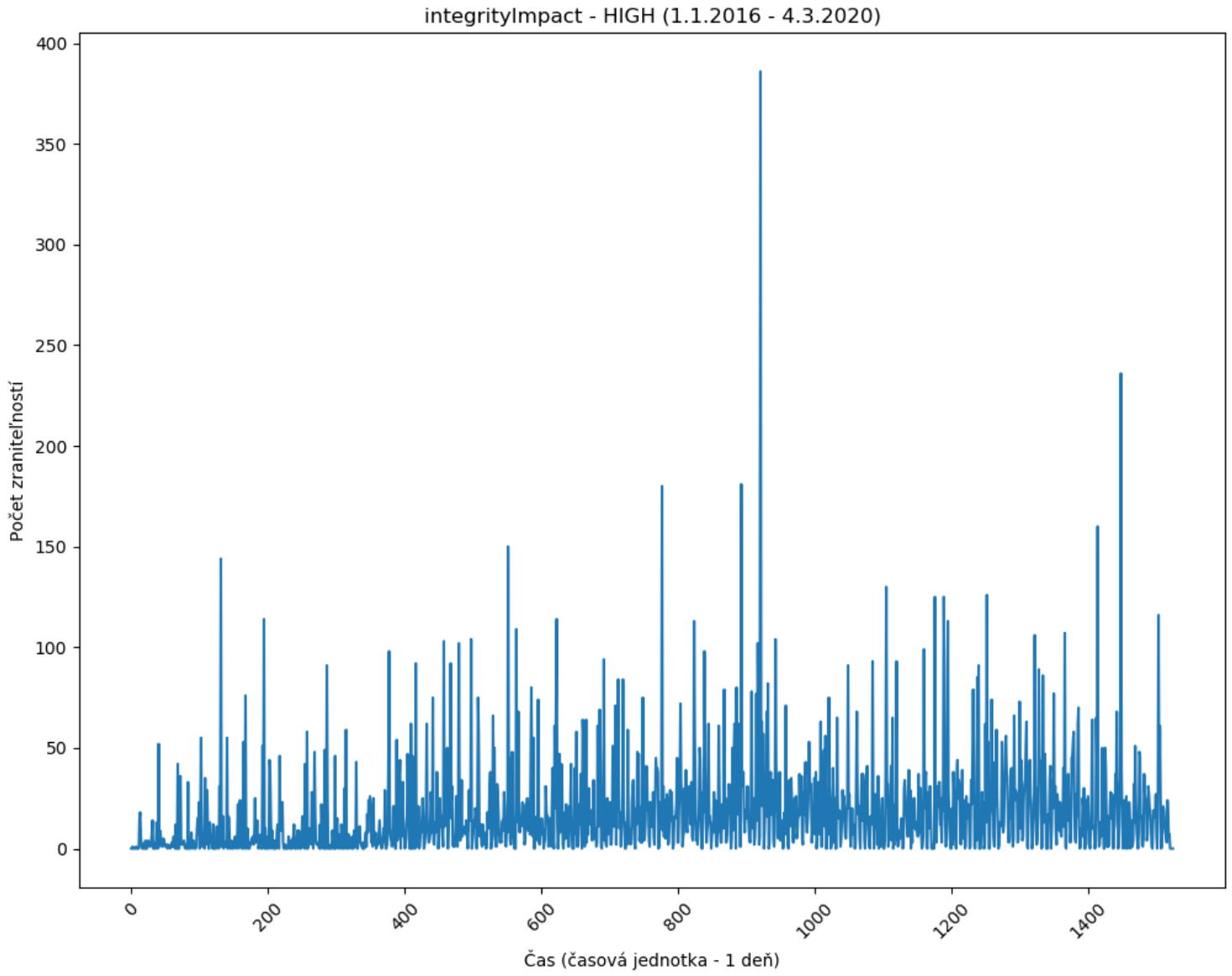
publishedDate	Date
id	CVE-YEAR-ID
attackVector	Network / Adjacent Network / Local / Physical
attackComplexity	Low / High
privilegesRequired	None / Low / High
userInteraction	None / Required
scope	Unchanged / Changed
confidentialityImpact	None / Low / High
integrityImpact	None / Low / High
availabilityImpact	None / Low / High
baseScore	0 - 10 (None / Low / Medium / High / Critical)
baseSeverity	None / Low / Medium / High / Critical
exploitabilityScore	0 - 10 (None / Low / Medium / High / Critical)
impactScore	0 - 10 (None / Low / Medium / High / Critical)

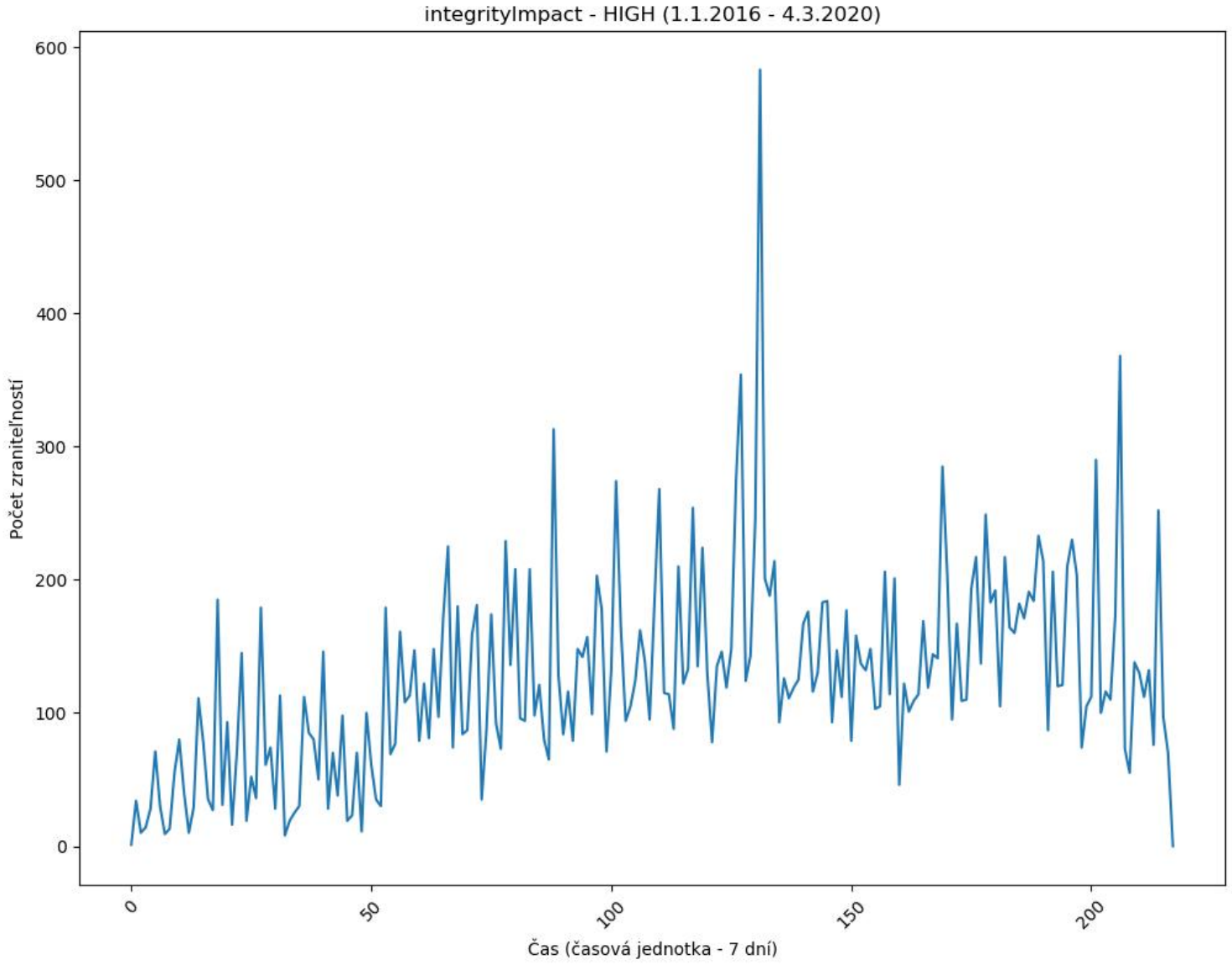

Counts of vulnerabilities, time unit: 7 days
Count of vulnerabilities
600
400
200
0
0
50
100
150
200
Time

integrityImpact	1 deň	2 dni	3 dni	4 dni	5 dní	6 dní	7 dní
NONE	18.04 %	6.96 %	1.97 %	0.52 %	0.98 %	0.39 %	0.92 %
LOW	25.92 %	12.6 %	5.91 %	2.89 %	1.97 %	1.18 %	1.83 %
HIGH	15.49 %	5.64 %	1.57 %	0.52 %	0.33 %	0 %	0.46 %

confidentialityImpact	1 deň	2 dni	3 dni	4 dni	5 dní	6 dní	7 dní
NONE	21.85 %	8.8 %	3.74 %	1.31 %	1.64 %	0.79 %	0.92 %
LOW	23.56 %	10.1 %	3.94 %	1.31 %	0.98 %	0.39 %	0.92 %
HIGH	14.64 %	4.99 %	0.98 %	0.26 %	0.33 %	0 %	0.46 %

availabilityImpact	1 deň	2 dni	3 dni	4 dni	5 dní	6 dní	7 dní
NONE	16.99 %	6.04 %	1.77 %	0.79 %	1.31 %	0.39 %	1.38 %
LOW	70.87 %	51.18 %	36.02 %	21.15 %	15.41 %	10.24 %	9.17 %
HIGH	13.89 %	4.59 %	0.98 %	0.26 %	0.33 %	0 %	0.46 %


integrityImpact - HIGH (1.1.2016 - 4.3.2020)
Počet zraniteľností
Čas (časová jednotka - 1 deň)
400
350
300
250
200
150
100
50
0
0
200
400
600
800
1000
1200
1400


integrityImpact - HIGH (1.1.2016 - 4.3.2020)
Počet zraniteľností
Čas (časová jednotka - 7 dní)
0
100
200
300
400
500
600
0
50
100
150
200

	attackComplexity_HIGH	attackComplexity_LOW	attackVector_ADJACENT_NETWORK	attackVector_LOCAL	attackVector_NETWORK	attackVector_PHYSICAL	availabilityImpact_HI	availabilityI	av
attackComplexity_HIGH	-								
attackComplexity_LOW	0,48	-							
attackVector_ADJACENT_NETWORK	0,28	0,51	-						
attackVector_LOCAL	0,49	0,67	0,37	-					
attackVector_NETWORK	0,54	0,95	0,45	0,45	-				
attackVector_PHYSICAL	0,09	0,37	0,24	0,32	0,28	-			
availabilityImpact_HIGH	0,57	0,92	0,52	0,76	0,84	0,36	-		
availabilityImpact_LOW	0,46	0,42	0,18	0,25	0,46	0,11	0,31	-	
availabilityImpact_NONE	0,49	0,92	0,42	0,49	0,93	0,3	0,71	0,44	-
baseScore_CRITICAL	0,33	0,72	0,39	0,4	0,72	0,2	0,77	0,2	0,54
baseScore_HIGH	0,56	0,92	0,48	0,64	0,89	0,3	0,87	0,31	0,86
baseScore_MEDIUM	0,51	0,89	0,45	0,62	0,86	0,38	0,79	0,55	0,86
baseScore_LOW	0,32	0,5	0,24	0,48	0,44	0,24	0,38	0,61	0,52
baseScore_NONE	-	-	-	-	-	-	-	-	-
baseSeverity_CRITICAL	0,34	0,72	0,39	0,4	0,72	0,2	0,77	0,21	0,55
baseSeverity_HIGH	0,59	0,92	0,48	0,66	0,89	0,3	0,88	0,31	0,86
baseSeverity_MEDIUM	0,51	0,89	0,45	0,62	0,86	0,38	0,78	0,55	0,86

AKTUÁLNY STAV

- Finalizácia datasetu o bezpečnostných udalostiach
- Finalizácia časových radov z bezpečnostných udalostí
- Skúmanie korelácií medzi jednotlivými radmi
- Predikcia

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

☺