nt konferenca 2021

27. – 29. september 2021

Nekega jutra, ko se zdani!

Milan Gabor

/me

- Etični heker
- Predavatelj
- Raziskovalec
- OWASP Maribor

Foreplay

- Bila je čudovita noč!
- Magnifico je špilal!
- Dokler ni prišlo do klica!
- Houston we have a problem!
- In potem se zdani, in…

Kje smo?

Se je kaj spremenilo?

2021 status – in ni še konec leta!

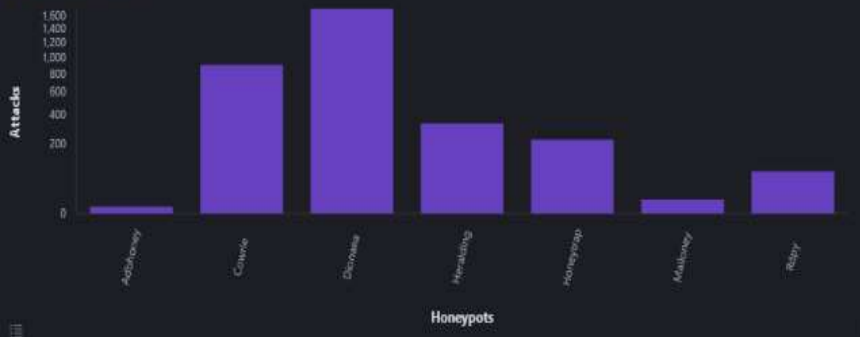
- Veliko dela za sistemske administratorje

- CVE-2021-26855
- CVE-2021-34473, CVE-2021-34523, CVE-2021-31207
- CVE-2021-34527
- CVE-2021-40444

Honeypot Attacks - Top 10

1,728	909	334	225	73	8	2
Dionaea - Attacks	Cowrie - Attacks	Heralding - Attacks	Honeytrap - Attacks	Rdpy - Attacks	Mailoney - Attacks	Adbhoney - Attacks

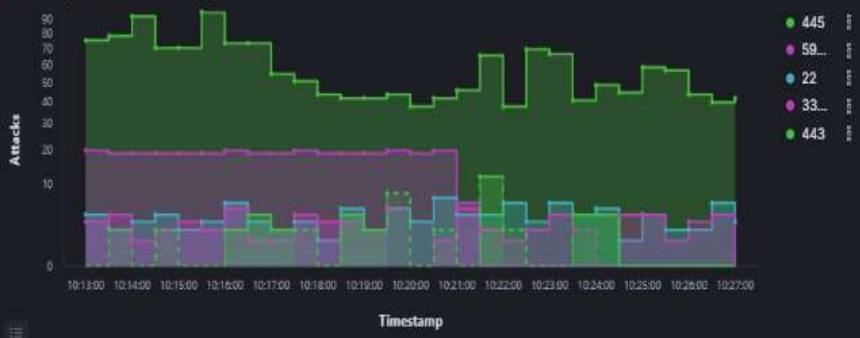
Honeypot Attacks Bar



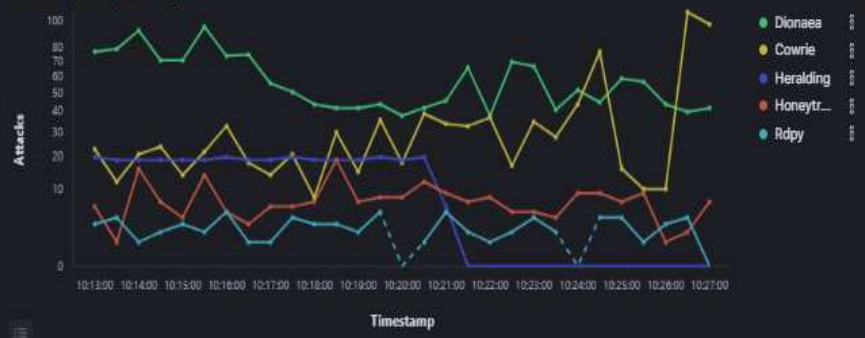
Honeypot Attacks Histogram

Honeypot Attack Map

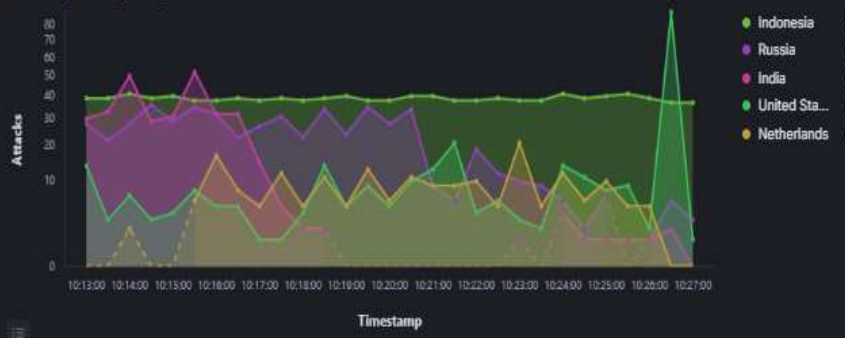
Attacks by Destination Port Histogram



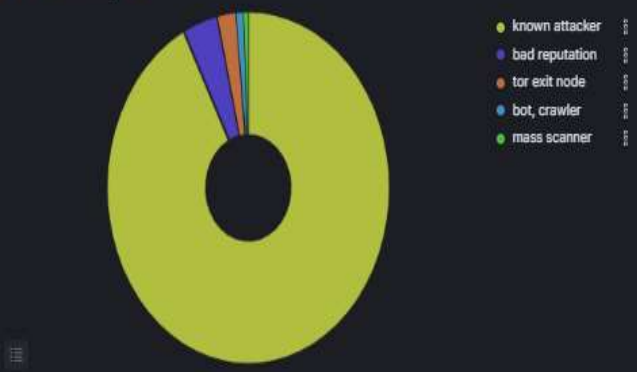
Attacks by Honeypot Histogram



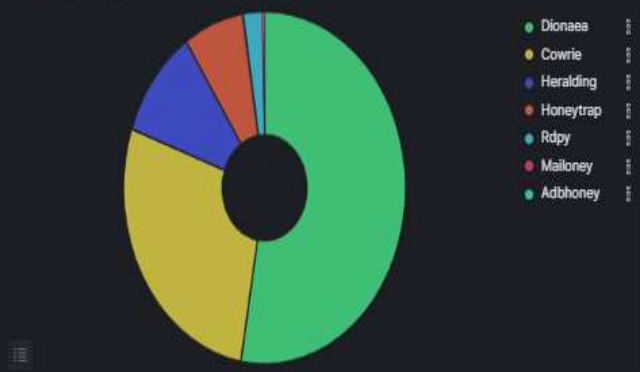
Attacks by Country Histogram



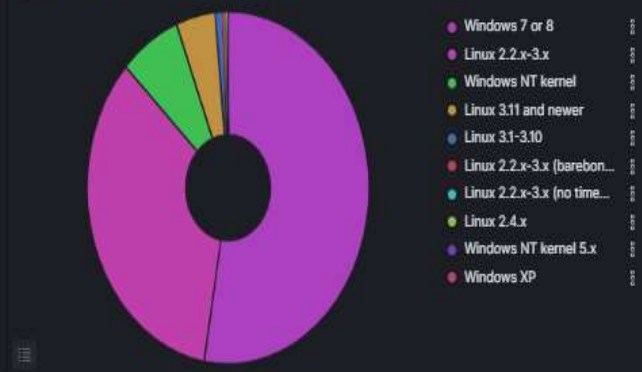
Attacker Src IP Reputation



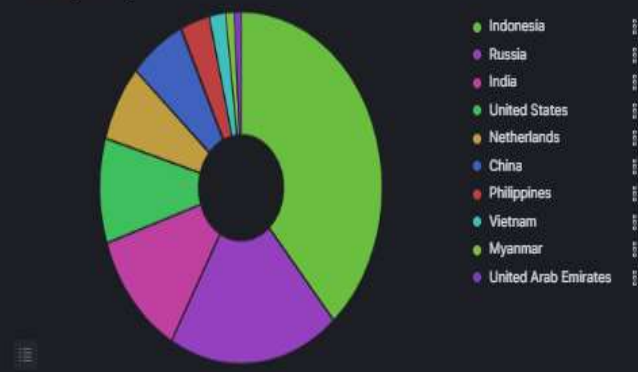
Attacks by Honeypot



P0f OS Distribution



Attacks by Country



Attacks by Country and Port

Suricata Alert Category Histogram

Se spomnite tega?

Računalniški sistem Lekarne Ljubljana ohromil izsiljevalski virus

Poslovalnice Lekarne Ljubljana izdajajo zdravila na papirnate recepte

Lekarna Ljubljana je bila v ponedeljek tarča napada izsiljevalskega virusa, ki je začasno onemogočil delovanje informacijskega sistema. Primer preiskuje policija, ponovna vzpostavitev sistema pa je v sklepni fazi.

1.5.8.3 IZVEDENI PROJEKTI S PODROČJA VARNOSTI IT

V letu 2020 je bil ključni poudarek na informacijski varnosti in razpoložljivosti ITK sistema. Vsa podana priporočila varnostnega pregleda iz leta 2019, se je v letu 2020 realiziralo oziroma pričelo z realizacijo rešitev:

1. VPN uporabnikom se je omejilo le na servise/storitve, ki jih potrebujejo za delo.
2. Uporaba deljenih gesel in tovarniških gesel je onemogočena.
3. Vklop podpisovanja komunikacij preko protokola SMB bo urejen z vpeljavo security hardeninga pravic na delovnih postajah do konca Q1 2021.
4. Izklopilo se je nepotrebne servise telnet.
5. Izklopilo se je šibki šifrirni protokol TLS 1.0.
6. Vpeljava zaščite dostopa do omrežja z 802.1x: infrastruktura urejena. Test v Lekarni Citipark uspešno opravljen. Projekt je v teku, predvideni zaključek v Q2 2021.
7. Deaktiviralo se je notranje lokalne administratorje.
8. Ustrezno se je konfiguriralo protivirusno zaščito.
9. SNMP community – privzeto geslo se je odstranilo.

Ob tem pa še:

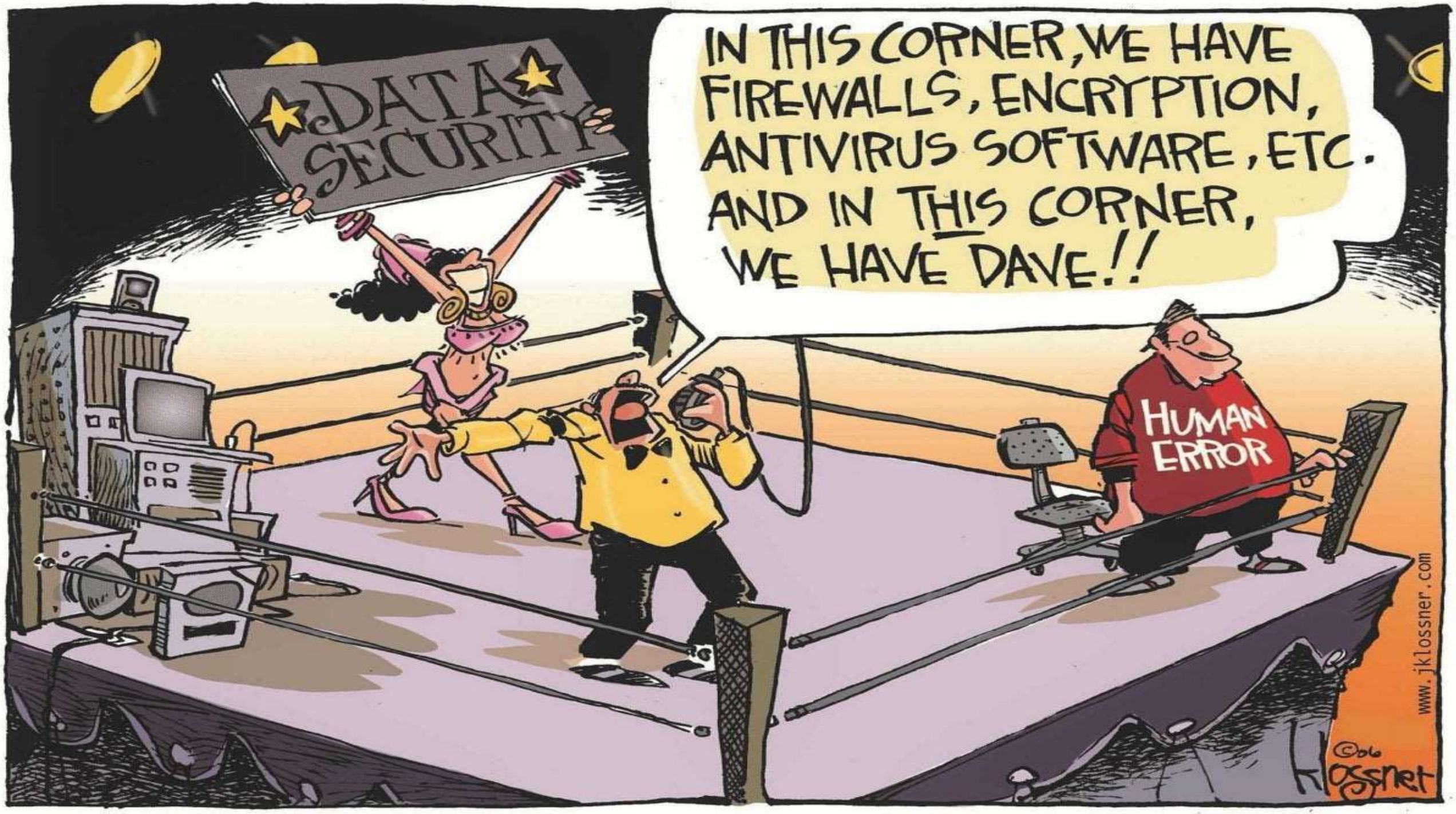
10. Segmentacija omrežja: v okviru izboljšanja varnosti znotraj internega omrežja Lekarne Ljubljana, so bili uvedeni dodatni mrežni segmenti za strežnike, uporabnike, tiskalnike in ILO-vmesnike.
11. Dodelava nadzora: v obstoječem nadzornem sistemu so bile pripravljene grafične sheme posameznih lokacij.
12. Oddaljena podpora za dlančnike: konec junija 2020 je bil zaključen projekt distribucije novih Androidnih dlančnikov po lokacijah in vpeljava orodja za pomoč na daljavo OneAssist.
13. Zamenjava nadzornega sistema za diskovno polje: postavitev novega sistema za nadzor diskovnega polja.
14. Implementacija enkripcije na vseh prenosnih računalnikih.

P2P zgodbe

- Zanimiv sogovornik včeraj
  - Navdušen nad AI rešitvijo
  - Vidi vse kar se dogaja
  - Celo nekaj, kar se mogoče ne bi smelo… Hmmm

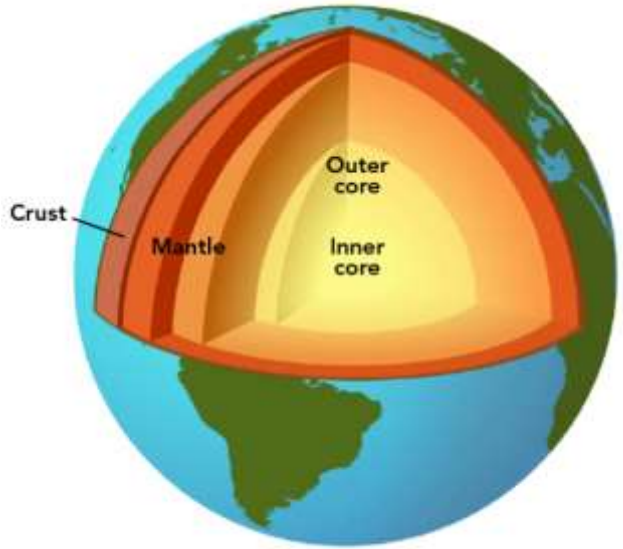
  - Cena je malce zunaj njegovega ranga..

  - Hint: Google SecurityOnion


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
©06 Klossner
www.jklossner.com

Ravni

- Sistem/domena/aplikacije
  - Prijave
  - Napačne prijave
  - Centralni logi
- Omrežje
  - Tokovi
- Oblak
  - O365 logi
  - Alarmi



Orodja

- Dobro je imeti arzenal orodij, ki nam lahko pomagajo
- Skenerji ranljivosti
- Domena
  - PingCastle
  - BloodHound
  - Elastic stack
- Logi
  - SIEM
    - Wazuh
    - Graylog
    - Sentinel za tiste z $$$
- Omrežje

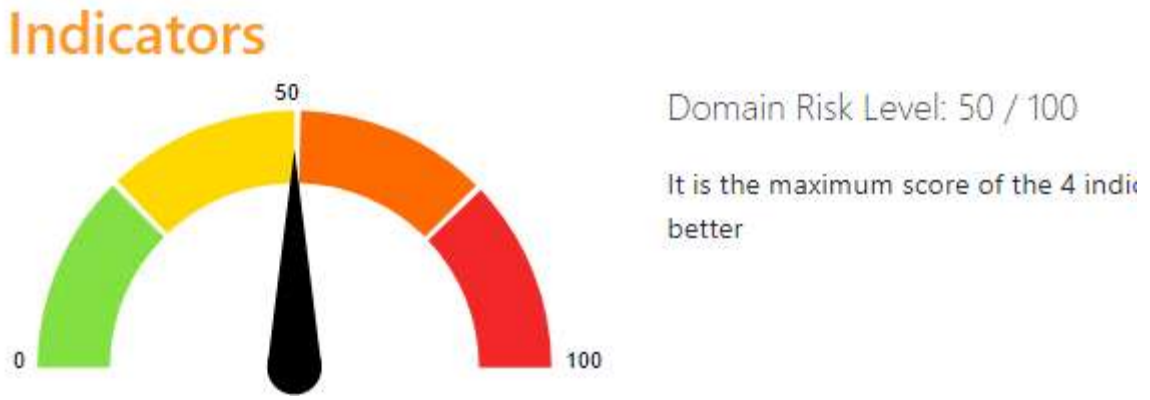
Elastiflow

Orodja

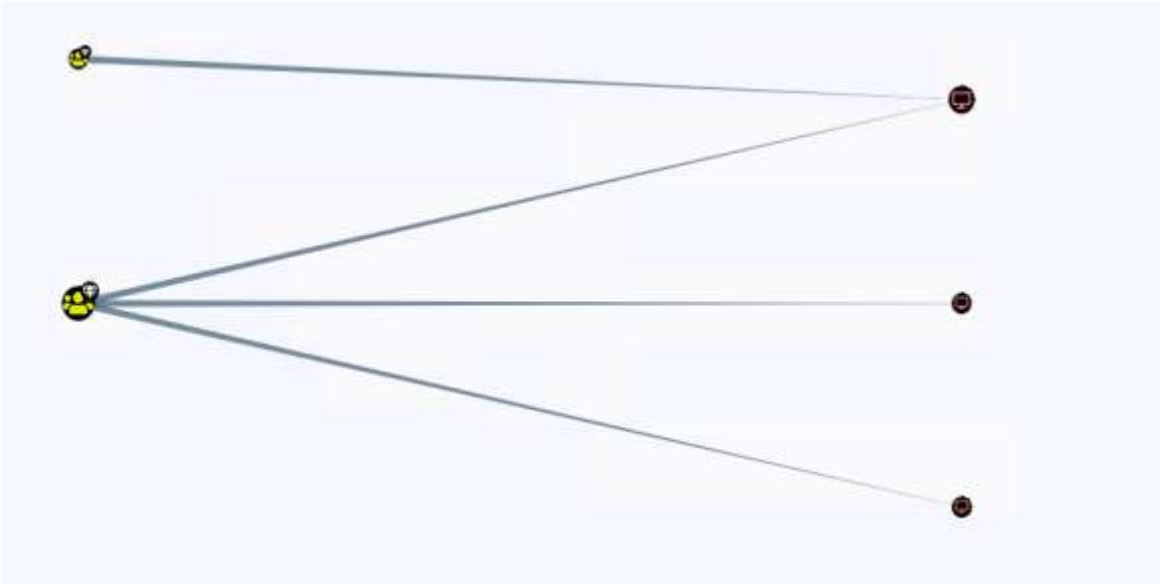
- Komercialna
  - $$$
  - Kaj izbrati?
  - Gartner
- Prostodostopna/Odprtokodna
  - Omejitve
  - Podpora

Analiza domene

- PingCastle
  - https://www.pingcastle.com/
  - Analiza domene v minuti
  - Stanje
  - Priporočila



- Bloodhound
  - https://github.com/BloodHoundAD/BloodHound
  - Kolektor za zbiranje podatkov
  - Lahko v intervalih
  - Graph oriented
  - Slabe konfiguracije



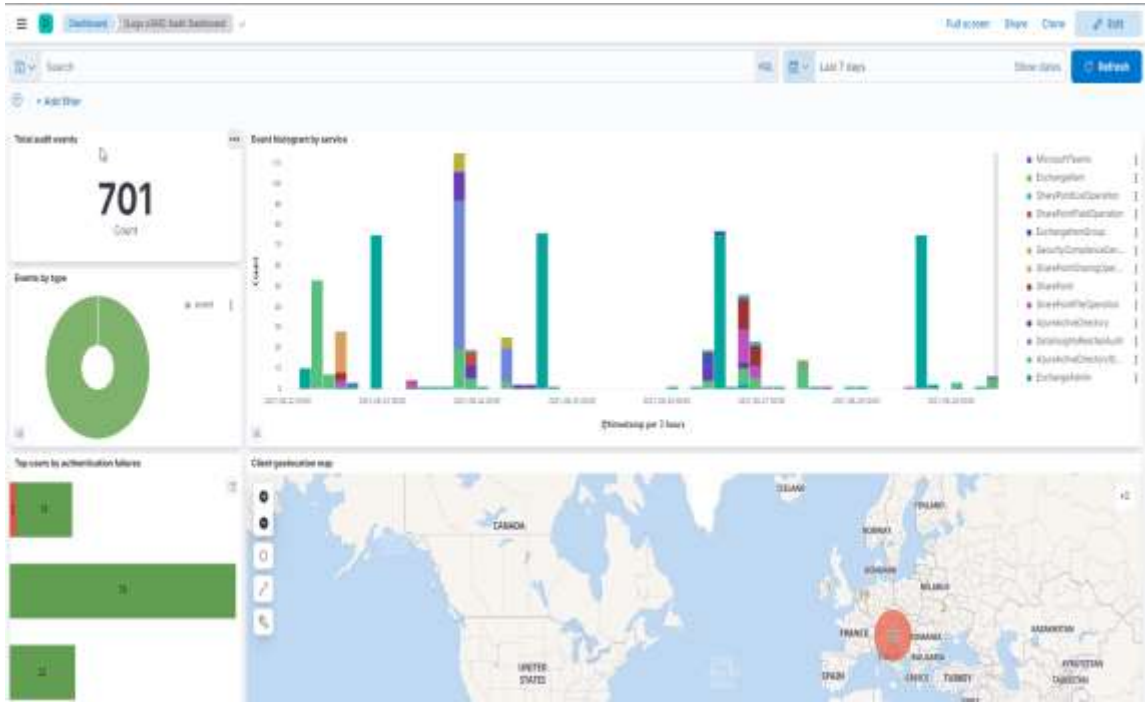
Demo

Wazuh

- Enostaven za setup
- Funkcije
  - Logi
  - Security dogodki
  - Poormans solution
  - Skladnost
  - Spremembe
- Agenti
  - Linux
  - Windows
- Elasticsearch v ozadju

Demo

O365 logi



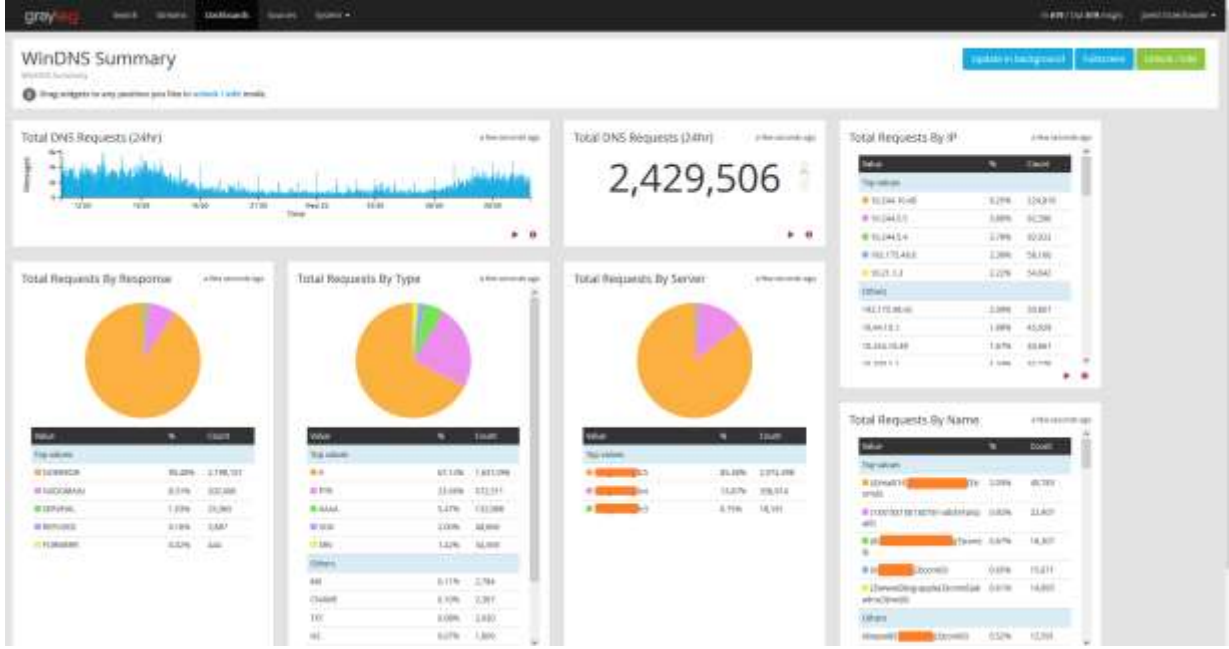
- Online
- Kdaj ste nazadnje šli kaj pogledat?
- Sentinel (licence, $$$)

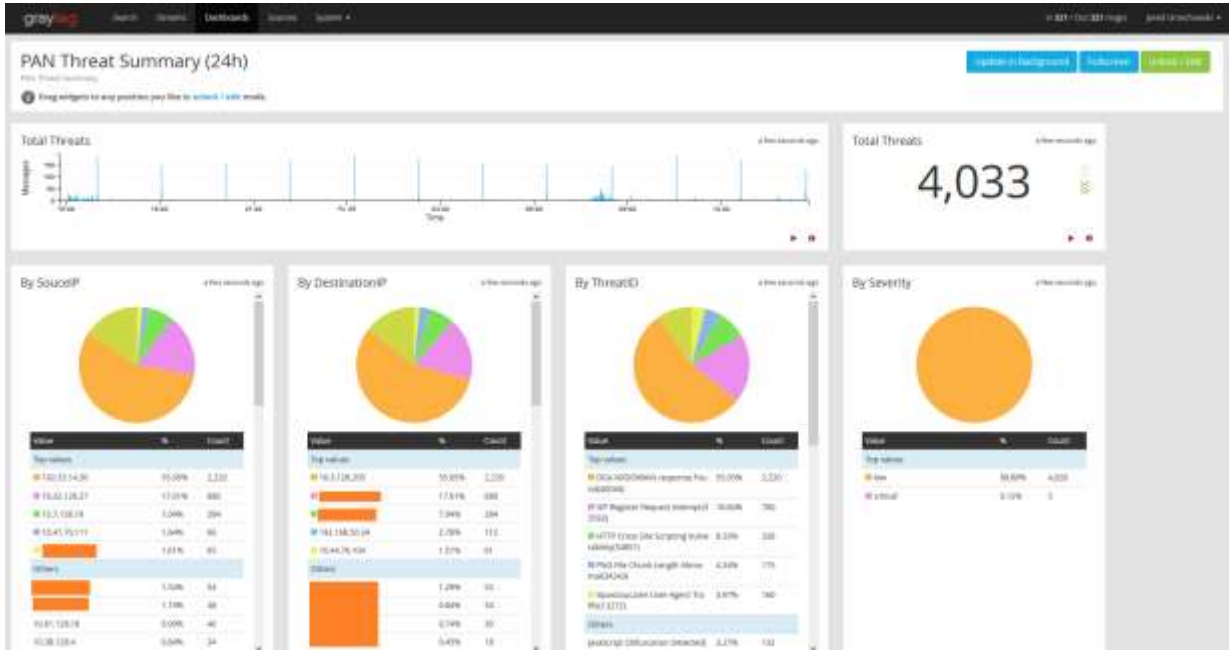
- Elastic stack?
- Beats O365 integration
- https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-o365.html

Demo

Graylog

- SIEM
  - On premise
  - V oblaku
  - Enostaven setup
  - Agenti
  - Syslog
- Enterprise funkcionalnost
- Omejitve
- Možnosti





Omrežje

- Flowi
- Kdo, kam, koliko

- Lahko pomagajo pri analizah
- Anomalije

- https://www.elastiflow.com/

Kaj danes potrebujemo? (minimalne zahteve)

- Napredni požarni zid
  - Pravila na uporabnika
  - Filter aplikacij, porti niso več dovolj
- EDR, XDR na delovnih postajah/strežniki
- Centralno logiranje
- SIEM
  - Corelation
  - Alerting
  - Retention time
- SOC(?)

- Človeka/ekipo, ki sistem upravlja

Domača naloga

- Onemogočite starejše/nepotrebne protokole ali funkcionalnosti (NETBIOS, LLMNR, IPv6)
- Vklopite podpisovanje (MITM)
- Vklopite dodatno logiranje (Power(S)hell)
- Preverite domeno (PIngCastle)
- Preverite domeno (BloodHound)
- Poglejte v loge v O365

https://lockedshields.si/

LOCKED SHIELDS 2021
TEAM SLOVENIA


Sharing
IS
Caring

MAY

Security

BE WITH

YOU

Hvala, da ste zdržali do konca!

@MilanGabor

nt konferenca
2021