TriOp
A new open-source tool for gathering (not just) security-related data from Shodan

Jan Kopřiva
jan.kopriva@alef.com  @jk0pr
ALEF CSIRT
How does the internet change over time?

• Quite an interesting question – how does the following change over time?
  • Number of internet-connected systems overall
  • Number of web servers supporting TLS 1.3
  • Number of systems vulnerable to BlueKeep
  • Number of internet-facing industrial control systems in UK
We all know Shodan...
...and Shodan gives us the answer (sort of)
All we need is to get the „count“ periodically

• Can be done manually each day, if you want data for only couple of searches
• For hundreds or thousands of searches we need a little automation
  • This is where TriOp comes in...
1. Provide/generate a list of searches
2. TriOp gets count for each search
3. TriOp exports/adds results to CSV
4. Repeat as necessary
What do we get?
How does it work?

Let’s take a look!
Main use cases

• Security researchers
  • How common are different vulnerabilities in different countries?
  • How common is SSL 2.0 in 2021?
  • ...

• (National) CSIRTs
  • How many vulnerable systems are in our constituency?
    • country:XX
    • asn:ASxxxxxxx
Want to use it?

https://github.com/NettleSec/TriOp or https://csirt.xyz
Thank you for your attention