



總務部



Z/OS FOR GENT
HACK THE MAINFRAME



Jonathan Prince

Senior Consultant at NVISO

Was a kid in the 80s

Owens an AS/400

Is building a Dalek

Shoutout

Phil Young & Chad Rikansrud

aka.

Soldier of Fortran
&
Bigendian Smalls

Authors of the Evil Mainframe course

The OGs of Mainframe Hacking



A detailed cyberpunk-style illustration of a futuristic underground city street. The scene is characterized by a dense network of pipes, conduits, and cables overhead, illuminated by vibrant neon lights in shades of magenta, cyan, and blue. The ground is wet and reflective, mirroring the colorful lights. On the right, a yellow and black striped hazard barrier is visible. The overall atmosphere is one of a high-tech, industrial, and somewhat gritty environment.

The last mainframe will be unplugged on March 15, 1996

Stewart Alsop - 1991



Stewart Alsop - 2002

A detailed, atmospheric illustration of a futuristic subway station. The scene is characterized by vibrant neon lighting in shades of pink, purple, and blue. The station has a tiled floor with large puddles reflecting the lights. On the left, a train is visible, its windows glowing with the same neon colors. The walls are lined with various panels, some featuring glowing circuit-like patterns. A sign on the right wall reads "STYLECP". The overall aesthetic is one of a high-tech, yet gritty, urban environment.

Myth #1

Mainframes are outdated, technological dinosaurs

Meanwhile, in the 60s...



IBM Z16

On-Chip AI processing

Quantum Safe

Up to 40TB of RAM

250Gb/s inter processor communication

Up to 19 billion business transactions/day

Availability level of seven nines

Tested withstand 8.0 earthquake



Statistics (2020)

90% of Credit Card transactions

77/100 Top Banks

All the Top 10 Insurers

71% of the Fortune 500

68% of the worlds IT workload

Market size of \$2.5 Billion in 2023, with a CAGR of 6.4% forecast until 2032



Myth #2

Mainframes are impenetrable digital fortresses



Why aren't Mainframes immune to compromise?

It's a computer.
Built by Humans.
Configured by Humans.
Maintained by Humans.
Used by Humans.



SHODAN

Explore

Downloads

Pricing [↗](#)

ikj56700a



TOTAL RESULTS

161

TOP COUNTRIES



United States 113

Japan 11

United Kingdom 9

Brazil 8

France 7

[More...](#)

TOP PORTS

992 108

23 49

1023 2

2223 1

8023 1



View Report



View on Map



Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [every](#)

188.165.59.84

ip84.ip-188-165-59.eu

OVH SAS

France, Lille

[IKJ56700A](#) ENTER USERID -

71.27.82.206

Comcast Cable Communications,
LLC

United States, Cranberry
Township

[IKJ56700A](#) ENTER USERID -

206.72.204.242

kvm143.is.cc

Interserver, Inc

United States, Secaucus

[IKJ56700A](#) ENTER USERID -

192.86.33.34

IBM

United States, Secaucus

SSL Certificate

[IKJ56700A](#) ENTER USERID -

Issued By:

| - Common Name:

Signing Certificate

| - Organization:

Cegep de Thetford

Issued To:

| - Common Name:

Server Certificate



SHODAN

Explore

Downloads

Pricing [↗](#)

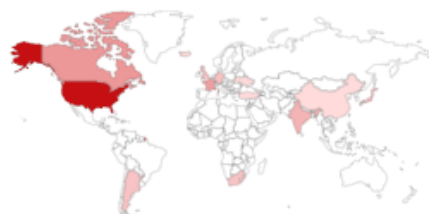
product:"IBM OS/390 ftpd"



TOTAL RESULTS

92

TOP COUNTRIES



United States	63
Canada	6
France	5
India	3
Argentina	2

[More...](#)

TOP PORTS

21	84
990	2
2021	2
2121	2
2345	1



View Report



View on Map



Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [everyth](#)

65.141.148.13

[CenturyLink Communications, LLC](#)

United States, Omaha

220-**FTPD1** IBM FTP CS V1R11 at bci-egig.baer-consulting.com, 11:07
220 Connection will close if idle for more than 10 minutes.
530-Error on __passwd() function call, errno=143, rsncode=090C05D0
530-The username is unknown
530 PASS command failed
214-The server-FTP commands are:...

192.86.32.87

[IBM](#)

United States, Secaucus

220-FTPSERVE IBM FTP CS V2R5 at S0W1.DAL-EBIS.IHOST.COM, 12:14:08
220 Connection will close if idle for more than 5 minutes.
530 PASS command failed
214-The server-FTP commands are:
214-ABOR,*ACCT,*ALLO, APPE, CDUP, CWD, DELE, FEAT, HELP, LANG, L
214-MODE, NLST, NO...

199.214.72.38

[goa2mvs.gov.ab.ca](#)

[Government of Alberta](#)

Canada, Edmonton

220-TCPFTP1 IBM FTP CS V2R5 at GOA2MVS.gov.ab.ca, 04:54:12 on 2024
220 Connection will close if idle for more than 5 minutes.
530 PASS command failed
214-The server-FTP commands are:
214-ABOR,*ACCT,*ALLO, APPE, CDUP, CWD, DELE, FEAT, HELP, LANG, L
214-MODE, NLST, NOOP, OPT...



Logica & Nordea

Well documented Mainframe compromise
Attributed to Gottfrid Svartholm a.k.a. anakata
Initial access via stolen credentials
Used 2 zero-day vulnerabilities
Developed exploits using Hercules Emulator



TOKYO

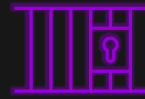
Challenges

Current Issues and the Future of Mainframe Security



Skill Gap

Experience is Retiring
New blood is limited
Steep Learning Curve



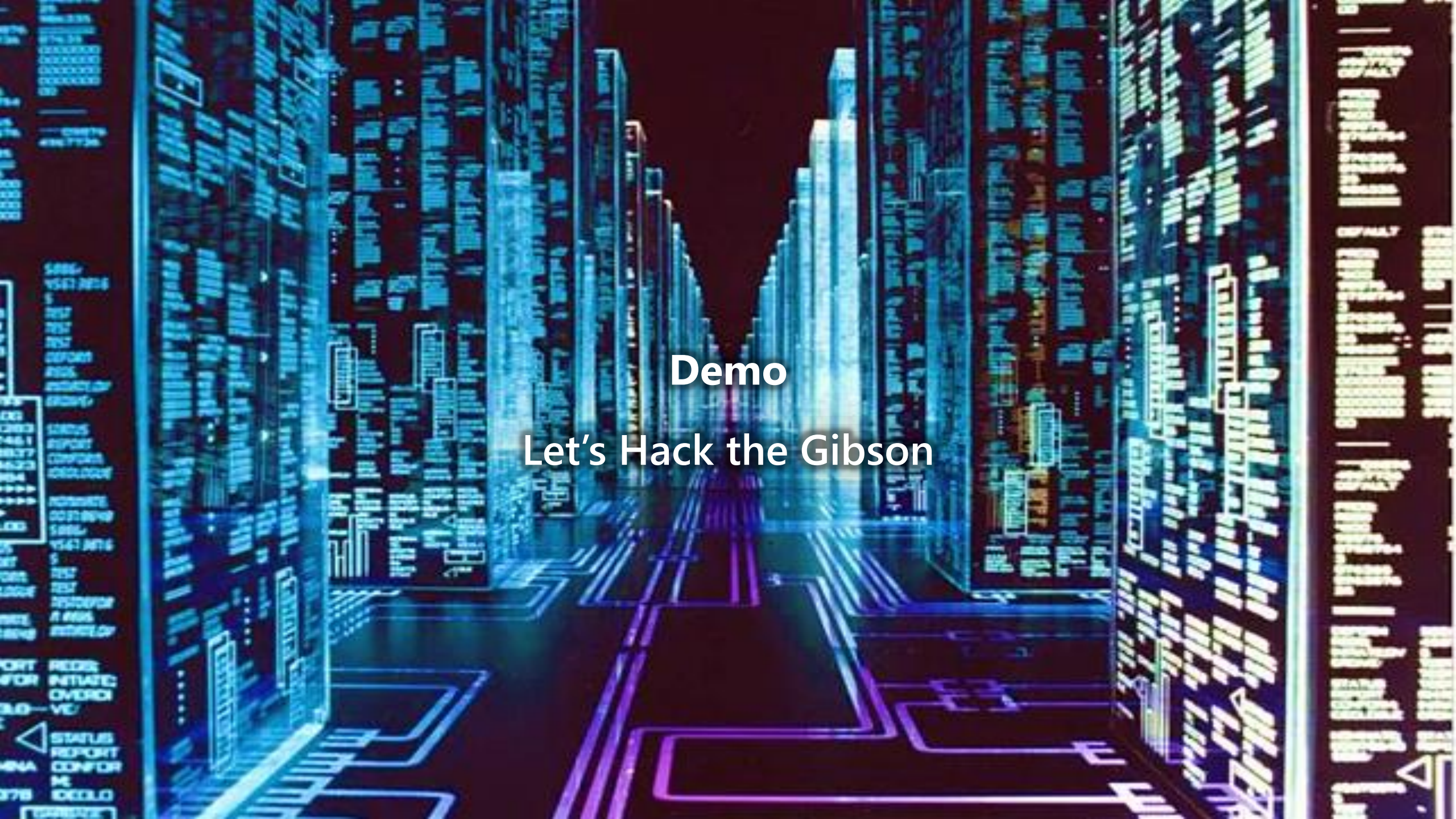
Approachability

Community
Access to z/OS
Limited Training



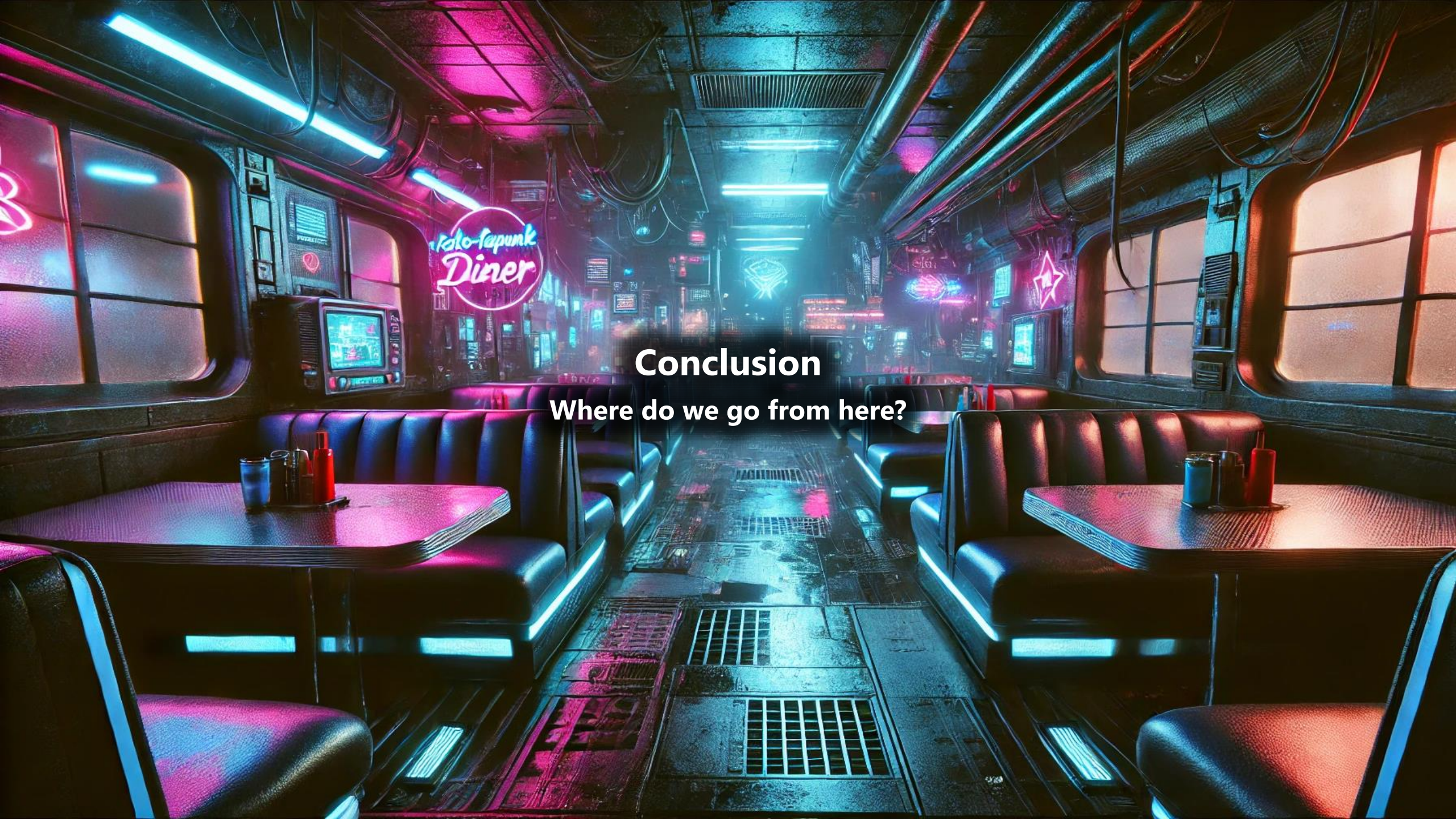
Oversight

Out-of-Scope
Testing Deficit
Perspective



Demo

Let's Hack the Gibson



Conclusion

Where do we go from here?




Learn Something
Different



Create and Build
Communities



Hack All the Things
(Hack the Planet?)



Thank you for your Attention

jonathan.prince@nviso.eu