LIFARS

your digital world, **secured**

IOC CHECKER

EXTERNAL NETWORK & INTERNAL NETWORK PENETRATION TEST DEVICE CONFIGURATION REVIEW

www.lifars.com

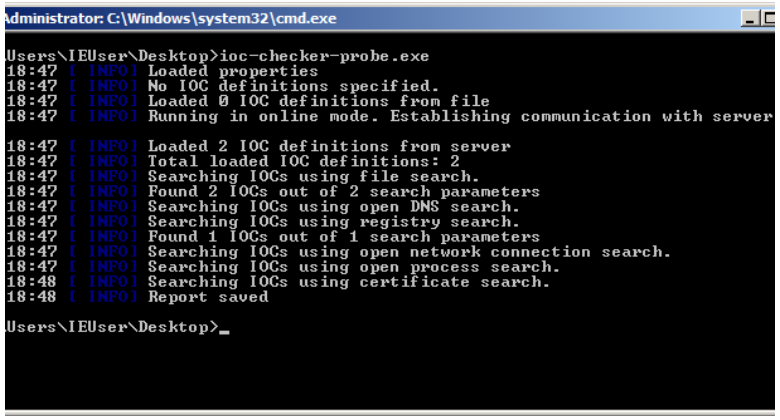
WHAT IS IT

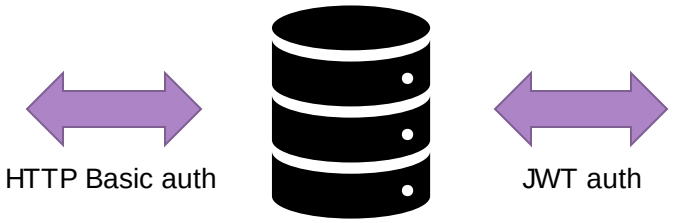
LIFARS
your digital world, secured

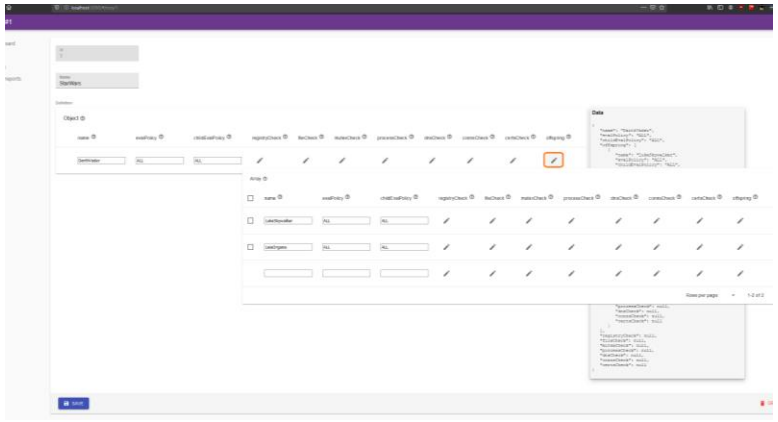
- Scans for indicators of compromise (IOCs)
- Full stack application
    - CLI client + Backend + Web admin console
- Our own IOC tree-based format
    - Can also convert from MISP & OpenIOC

APPLICATION STACK

LIFARS
your digital world, secured







IOC Probe (CLI client)

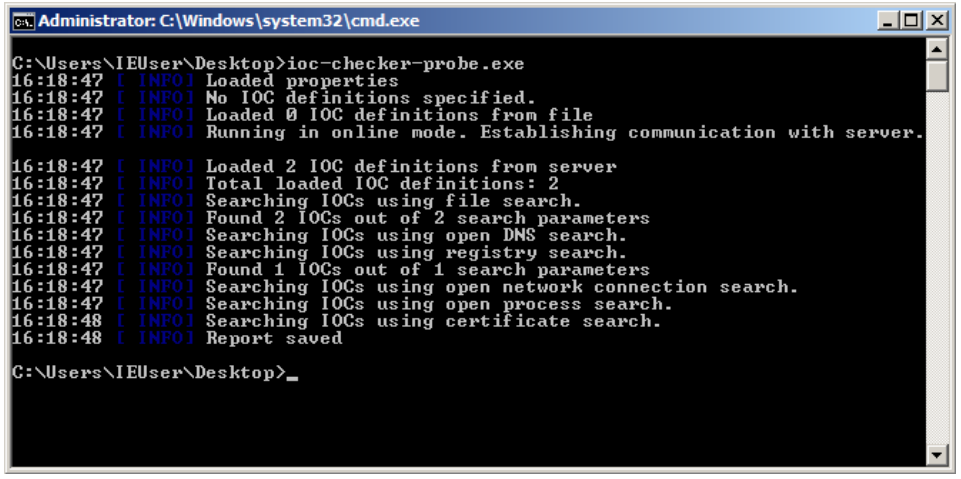
Server

IOC Admin

IOC PROBE

LIFARS
your digital world, secured

- Small CLI utility (2.5 MB) deployed on a client machine
  - Written in Rust
  - Fully native app, no external dependencies
- Downloads IOCs from server and checks if some is present
- Afterwards uploads result on server
- Supports also **offline** mode – no connections from server
  - IOC definitions are specified manually (JSON format)



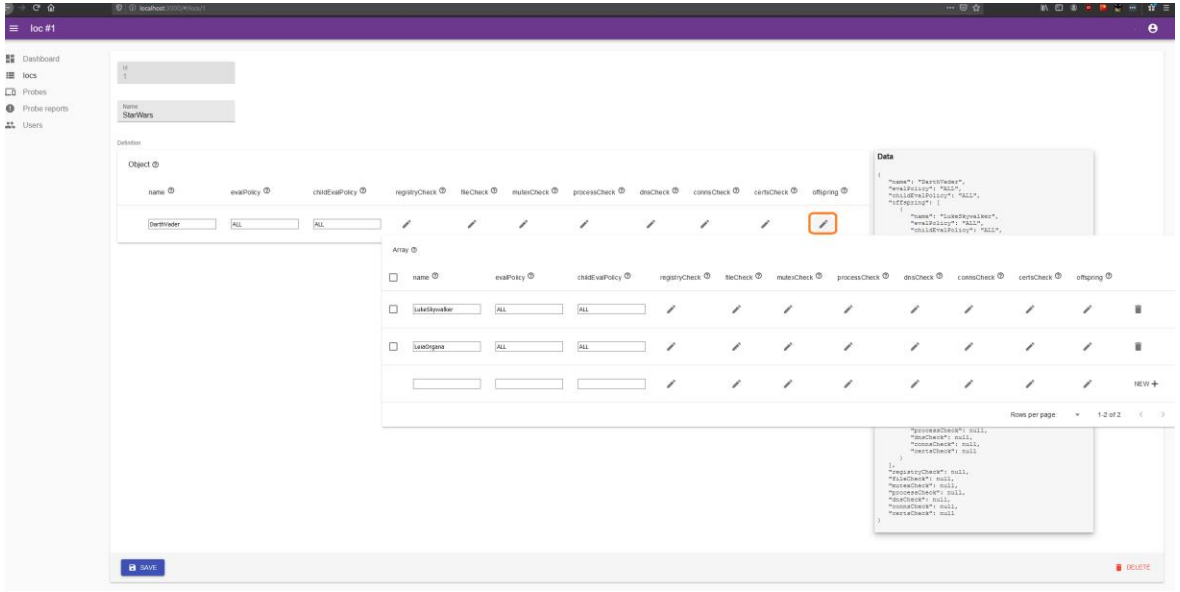
IOC PROBE

- Able to detect IOCs by
  - File name
  - File using MD5, SHA1 & SHA256 hash
  - Running process name
  - Windows Registry
  - DNS address
  - Network connection
  - Certificate name
  - Process mutex
- Supports also regex search

IOC ADMIN

LIFARS
your digital world, secured

- It can
  - Manually create/edit IOC definitions (on image)
  - Register new probe access tokens
  - View scan reports
  - Manage feed sources for externally defined IOCs
    - Periodically downloads new IOCs
    - MISP & OpenIOC formats supported ATM



THANK YOU

LIFARS

your digital world, **secured**

QUESTIONS?