

X33fcon workshop – module 3 operational oversight

⚡ PowerUp Red Team Ops with RedELK ⚡

Lorenzo Bernardi
Marc Smeets
May 2023

x33f con

When Red meets Blue...

OUTFLANK

clear advice with a hacker mindset

Module 3

Operational Oversight

INDICES

RedELK has the following main indices:

- `rtops-*` : all implant logs
- `redirtraffic-*` : all traffic logs
- `Credentials-*` : list of all credentials harvested
- `implantsdb` : list of all implants

<https://github.com/outflanknl/RedELK/blob/master/example-data-and-configs/RedELKFieldnamesV2.md>

INDICES

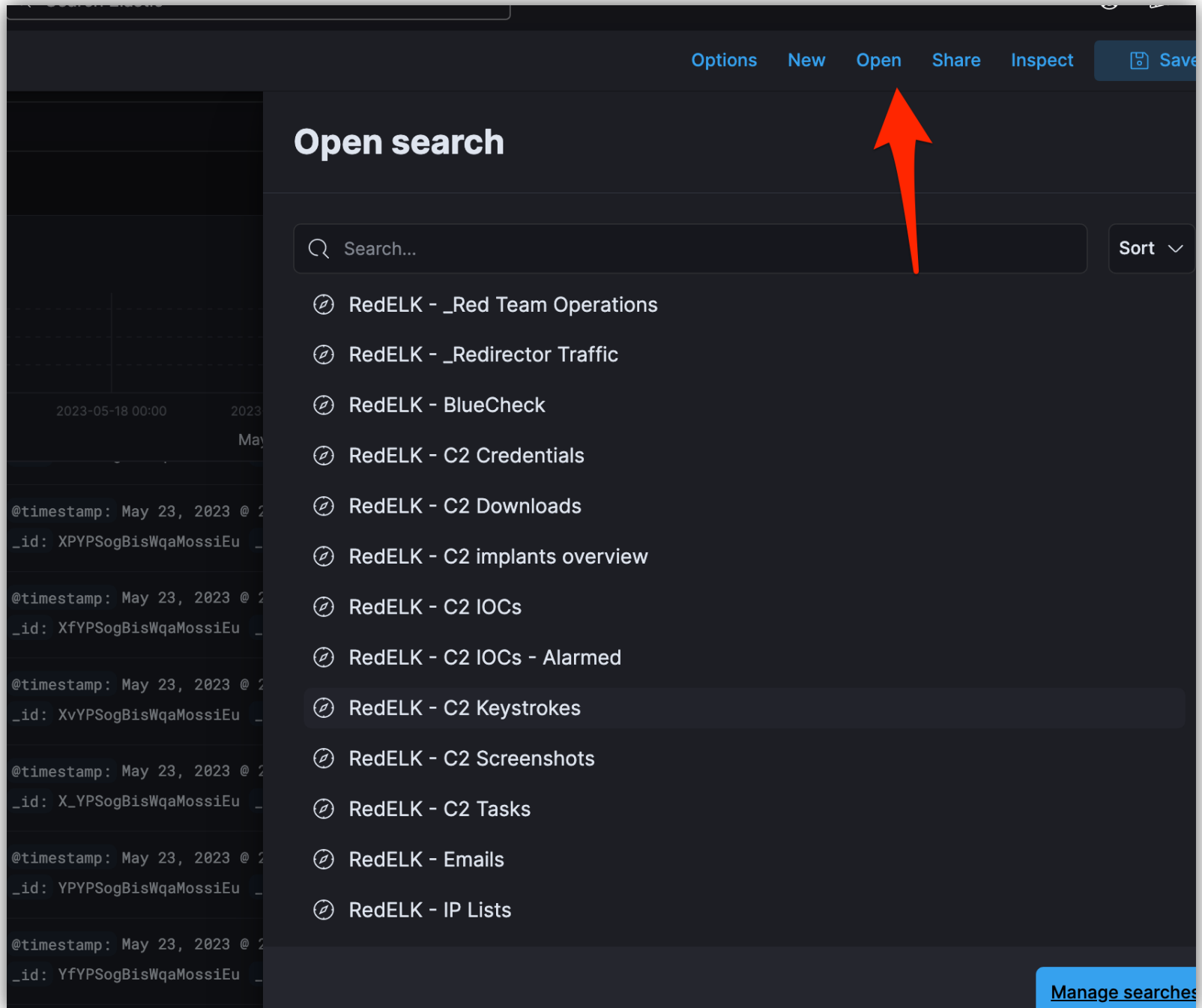
Secondary indices:

- Email-* : ingested emails (beta)
- bluecheck : index with data resulting data from blueteam checks, e.g. domain classification

Background indices – no need to mess with these:

- Redelk-*
- Redelk-domainlist-*
- Redelk-iplist-*
- .siem-signals-*

VIEWS



EASE OF USE

Pre made views and easy insight of:

- implant/beacon logs, including enrichments
- redir traffic, including lots of enrichment
- All implants, plus link to full raw log files
- Downloaded files, plus link to full files
- Screenshots, thumbnail and link to full picture
- Keystrokes
- IOCs as reported by Cobalt Strike
- In the RedELK left side menu:
 - link to mitre attack
 - Neo4j browser
 - Jupyter notebook

BACKGROUND PROCESSES

Enrichment of data in indices by Logstash – on ingest time:

- GeolP
- Ruby scripts for hyperlinks in Kibana views, e.g. screenshots, implant logs
- Parsing log lines and duplicating for other indices, e.g. implantdb

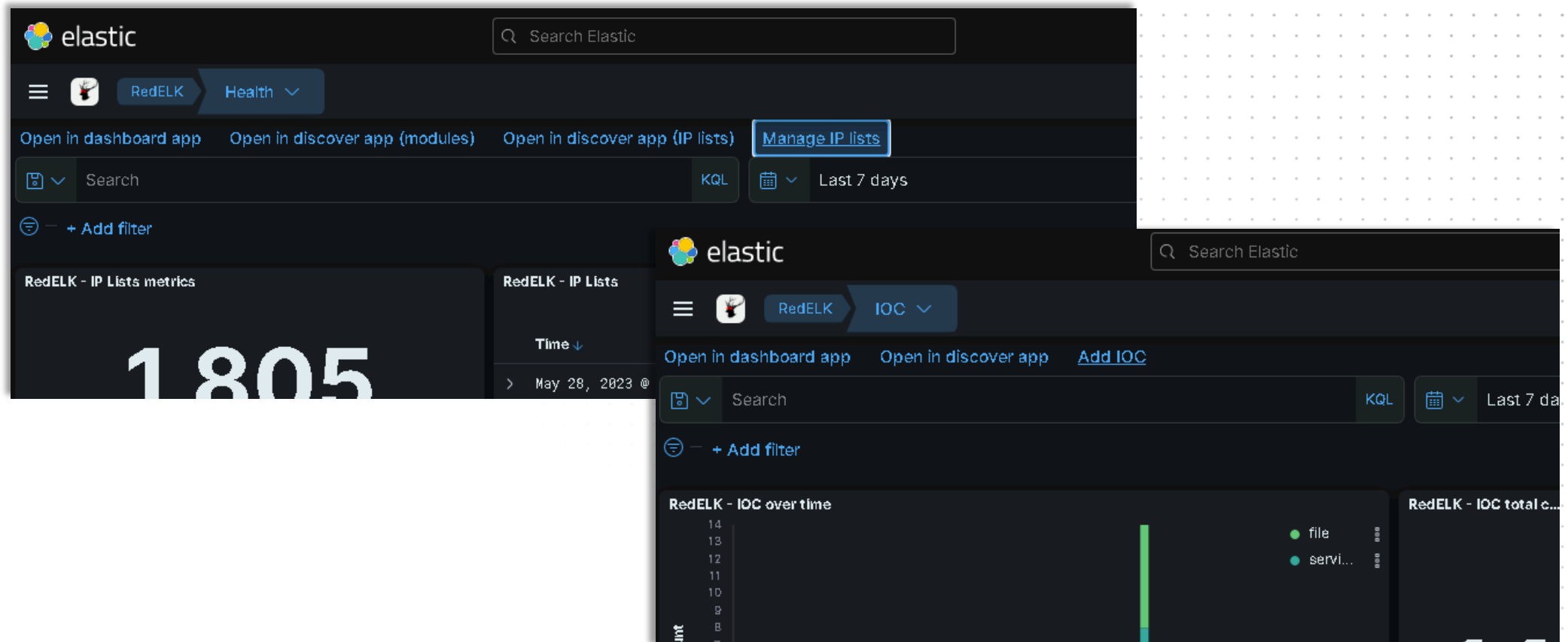
Background scripts:

- Enrichment: implant data, greynoise, domain classification, tor
- rsync to c2 servers and copying relevant files to RedELK server
- Make thumbnails

KIBANA APP

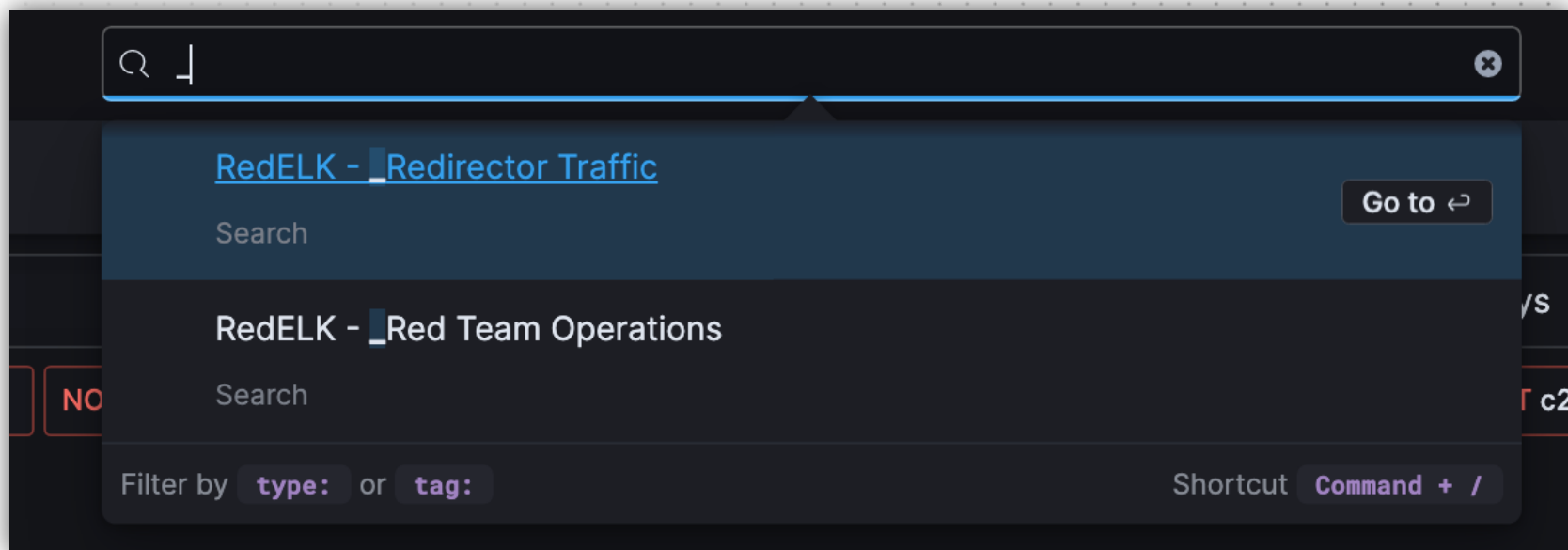
Wrapper for all dashboards +:

- IP lists management
- IOC management



TRICK - SEARCH IN SEARCH

See that _ !





LAB 3

Operational Oversight

1. Run multiple implants from multiple lab systems
2. Use RedELK to get insight into the data

Lorenzo Bernardi & Marc Smeets

lorenzo@bernardi.be

marc@outflank.nl