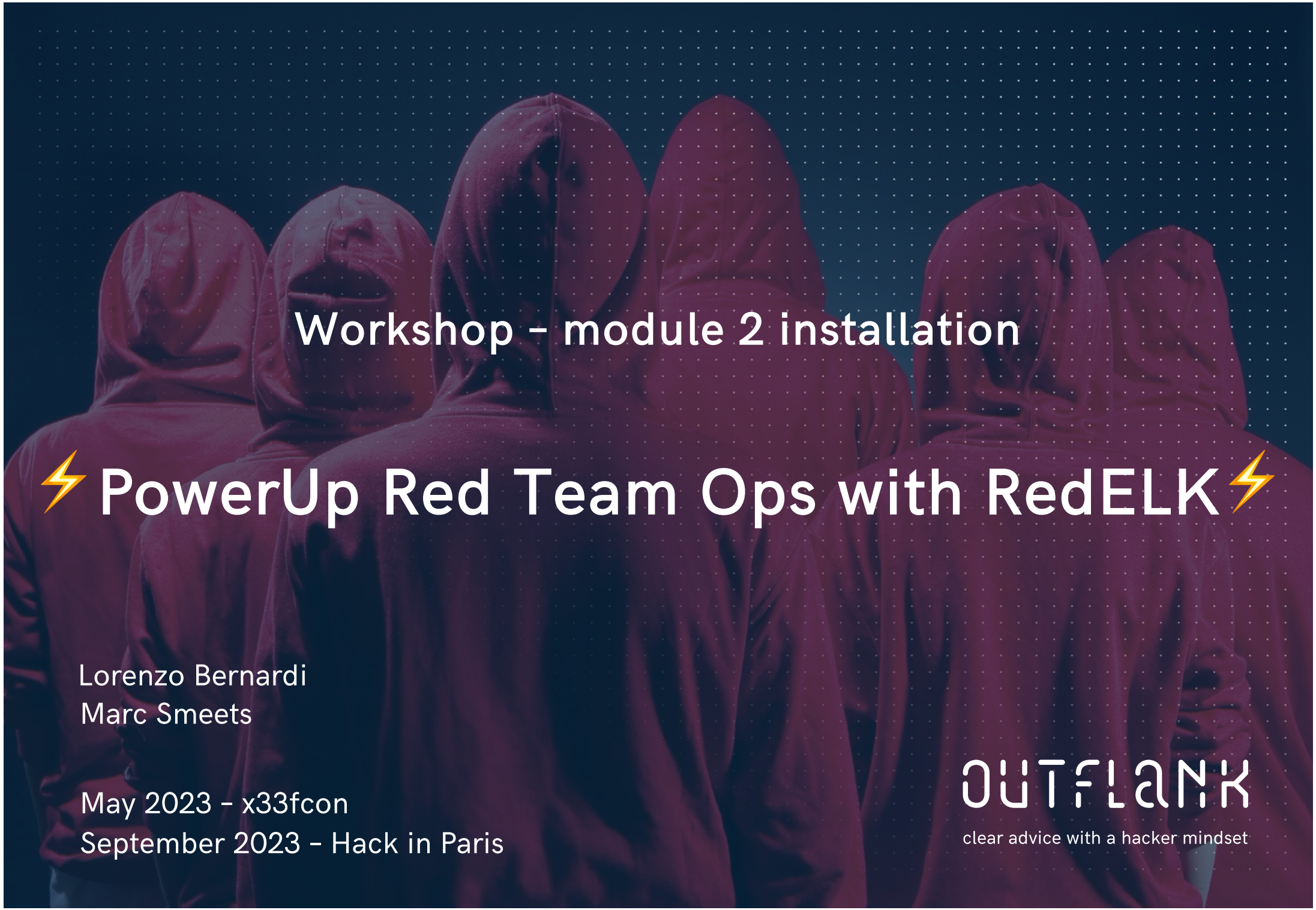


Workshop - module 2 installation

PowerUp Red Team Ops with RedELK

Lorenzo Bernardi
Marc Smeets

May 2023 - x33fcon
September 2023 - Hack in Paris

OUTFLANK
clear advice with a hacker mindset

Module 2

RedELK installation

SYSTEM REQUIREMENTS

Overall:

- only apt based systems are supported

RedELK server:

- Dedicated system
- 8GB, ideally 16GB of ram. Moderate CPU. Disk space at least 50GB.
- Needs to have a TCP port reachable for the redirs and teamservers for inbound filebeat traffic.

Redirector:

- Insignificant memory and disk

C2 server:

- Insignificant memory and disk. RedELK server needs to be able to setup a ssh/rsync connection to your C2server.

SUPPORTED RED TEAMING SOFTWARE

C2 servers	
Cobalt Strike	Full support
Outflank Stage1	Full support
PoshC2	Basic support (only implant logs, no screenshots, etc)
Sliver, Covenant, Mythic	In development, you can help!

Redirectors	
HAProxy	Full support – requires modified logging format
Apache	Full support – requires modified logging format
Nginx	Full support – requires modified logging format
RedWarden	In development

REDELK INSTALLATION

Overall flow:

1. Prepare your red teaming infra with proper naming and config
2. Generate installation package
3. Run installation package on redirectors
4. Run installation package on C2 servers
5. Run installation package on RedELK server

REDELK INSTALLATION - 1 PREPARE

Naming convention

- `filebeatID`: the name entered during installation should match the cron config file
- `Attackscenario`: common name shared amongst components
- Redirector `backend` name: need to start with "c2", "decoy" or "alarm"
- Redirector `frontend` name: no space

https://github.com/outflanknl/RedELK/wiki/Naming-requirements-within-RedELK

REDELK INSTALLATION – 1 PREPARE

Logging

- By default, reverse proxies do not provide sufficient logging.
- Modify the setup to include things like name of frontend and backend, x-forwarded-for info, headers

Without this level of detail, traffic logging is almost useless and RedELK can't generate certain alarms for you.

More info here:

https://github.com/outflanknl/RedELK/wiki/Redirector-installation

https://github.com/outflanknl/RedELK/tree/master/example-data-and-configs

REDELK INSTALLATION - 2 INSTALL PACKAGE

One time per RedELK install - generate installation packages:

- Modify `certs/config.cnf`
  - Important to use the correct IP and DNS info
  - Used for SSL keys for comm between c2 and RedELK servers
- Run `initial-setup.sh certs/config.cnf`
- Out come installation packages:
  - `c2servers.tgz`
  - `redirs.tgz`
  - `elkserver.tgz`

https://github.com/outflanknl/RedELK/wiki/Generating-keys-and-packages

REDELK INSTALLATION - 3 REDIRECTORS

In short

- On your redir extract `redirs.tgz`
- Run:

```
install-redir.sh $FileBeatID $ScenarioName $RedELKIP:Port
```

Debugging

- Output in `redelk-install.log`
- `Filebeat` logs

https://github.com/outflanknl/RedELK/wiki/Redirector-installation

REDELK INSTALLATION - 4 C2 SERVER

In short

- On your C2 server extract `c2server.tgz`
- Run:

```
install-x2server.sh $FileBeatID $ScenarioName $RedELKIP:Port
```

Debugging

- Output in `redelk-install.log`
- `Filebeat` logs
- Background running scripts log to `/var/log/redelk/*`

https://github.com/outflanknl/RedELK/wiki/C2-server-installation

REDELK INSTALLATION - 5 ELKSERVER

In short

- On your RedELK server extract `elkserver.tgz`
- Run installer `install-elkserver.sh`. Optional parameters:
  - `limited` (no Neo4j and no Jupyter), `dryrun` (only pre-install checks), `fixedmemory` (ES and Neo4j to 1GB), `dev` (dev mode, rebuilds containers and has test data)
- Define C2 servers in `mounts/redelk-config/etc/crond.d/redelk`
- Post install config - more on this in module 4

Debugging

- Output in `redelk-install.log`
- `docker logs redelk-$container`
- Script logs stored in `mount/redelk-logs/*`

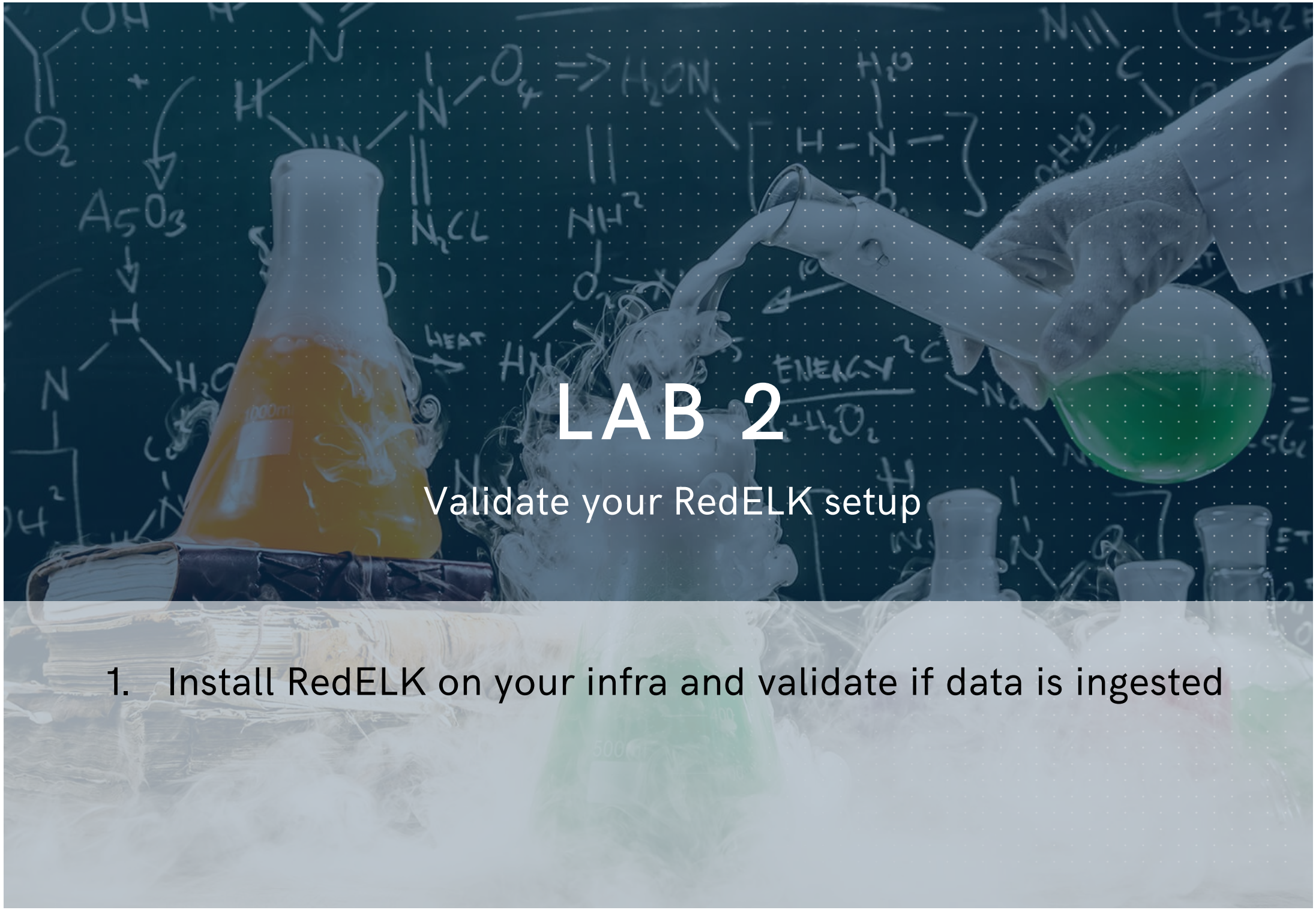
https://github.com/outflanknl/RedELK/wiki/RedELK-server-installation

REDELK INSTALLATION – THE ANSIBLE WAY

Optional installation process

- RedELK client and servers can be installed through Ansible

https://github.com/fastlorenzo/redelk-ansible



LAB 2

Validate your RedELK setup

1. Install RedELK on your infra and validate if data is ingested

Lorenzo Bernardi & Marc Smeets

lorenzo@bernardi.be marc@outflank.nl