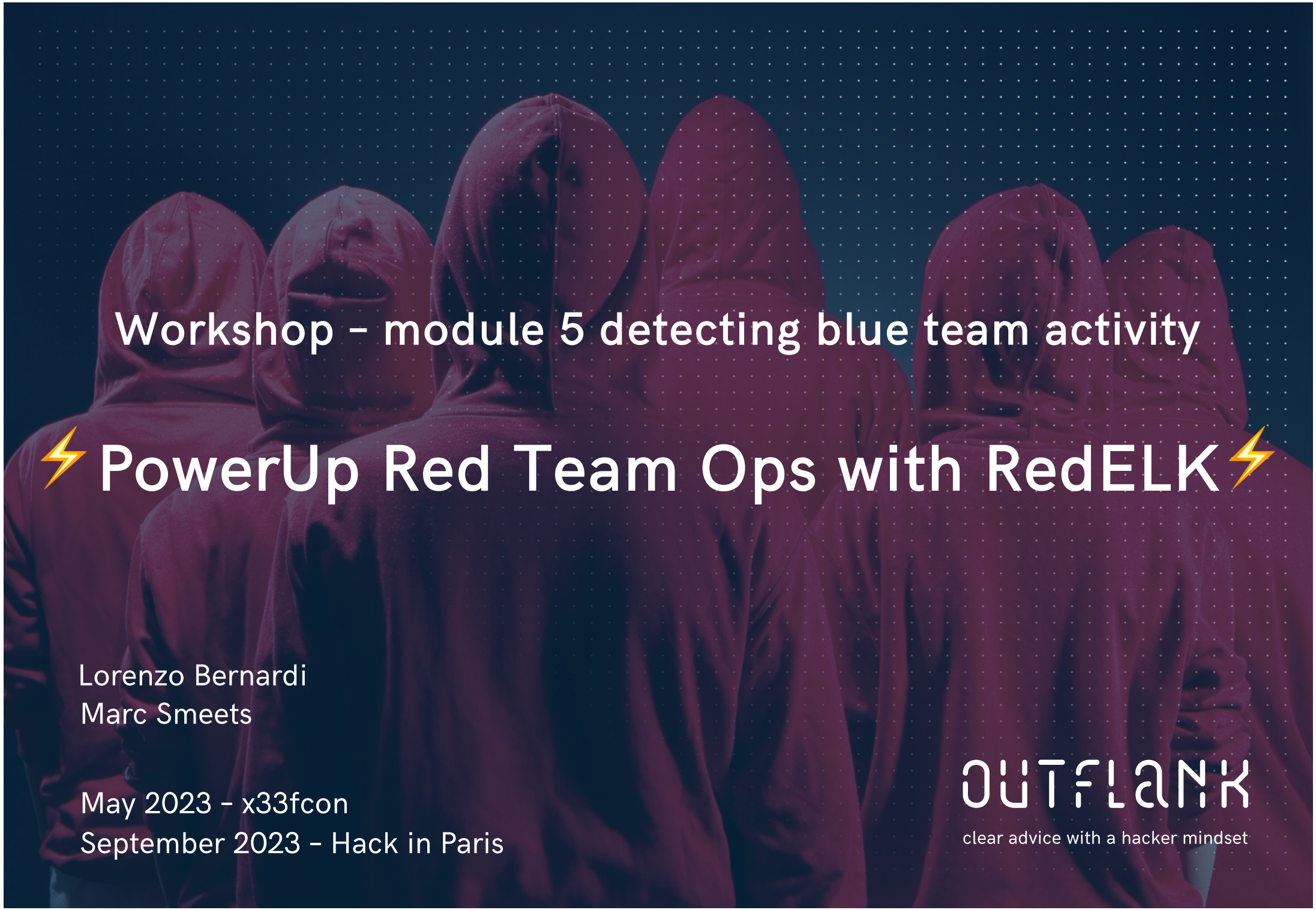


Workshop - module 5 detecting blue team activity

⚡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 5

Detecting blue team activity

OVERVIEW OF ALARMS

Alarms currenlty supported by RedELK:

- **alarm_filehash**: alarms SHA/MD5 hashes of your uploaded files that are also found on VirusTotal, IBM X-Force and/or Hybrid Analyses. Requires API key per provider. If you leave the API key empty the check is not performed.
- **alarm_httptraffic**: alarms IP's that aren't listed in any iplist* but access redirector backends named c2*.
- **alarm_useragent:** alarms User-Agents that are listed in config file blacklist_useragents.conf but access redirector backends named c2*.
- **alarm_backendalarm**: alarms any traffic hitting a redirector backend named *alarm*.
- **alarm_manual**: alarms if a C2 message contains the text REDELK_ALARM. This is useful for testing if your alarm setup works. Type REDELK_ALARM something something in your C2 either in the event log or in the implant to test.
- **alarm_dummy**: only used for testing purposes, probably no need to enable.

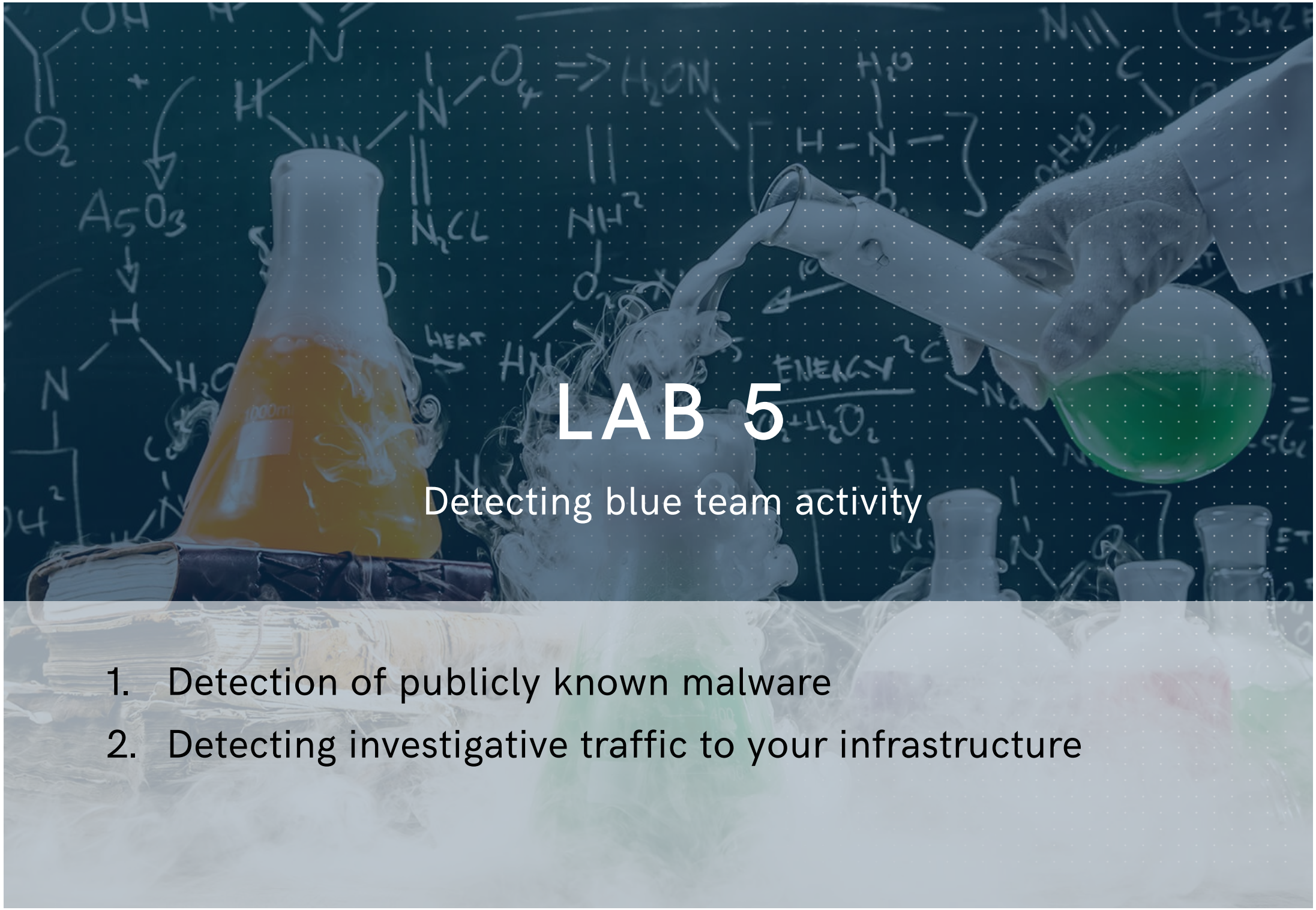
TECH STUFF ON ALARMS

Enabling and config:

- **Main config file:** `mounts/redelk-config/etc/redelk/config.json`
- **IP config files**: `mounts/redelk-config/etc/redelk/iplist files*`

Underlying logic of the modules:

- Check the modules in the redelk-base container. These are put in place during install. The source can be found here: `docker/redelk-base/redelkinstalldata/scripts/modules/*`



LAB 5

Detecting blue team activity

1. Detection of publicly known malware
2. Detecting investigative traffic to your infrastructure

Lorenzo Bernardi & Marc Smeets

lorenzo@bernardi.be marc@outflank.nl