SAIBERSOC: Synthetic Attack Injection to Benchmark and Evaluate the Performance of Security Operation Centers

ACSAC 2020

Martin Rosso, Michele Campobasso, Ganduulga Gankhuyag, Luca Allodi

Department of Mathematics and Computer Science, Security Group
Two phases:

- **Attack identification:**
  Tier-1 SOC analysts

- **Attack investigation:**
  Higher tiers (i.e., ≥ 2)

**SOC performance:**
We do not know attacks in advance
Experiment

> Validation

Classroom
(124 students, 63 groups)

identify & investigate attacks

Inject normal network traffic

Inject two attacks

GOODSOC

BADSOC

Fill in

SOC report

Us
Experimental Validation

> Simulated Attacks: Raised alerts

Mirai alerts

Exim alerts
Experimental Validation

> Simulated Attacks

Command and Control Server

victim

reconnaissance

compromise
Results:

> Attack identification

Figure 4: Attack identification by reported scenario.
Results:

> Attack investigation

**Mirai attack**

- **BADSOC (n=10)**: 7, 5, 6
- **GOODSOC (n=12)**: 9, 5, 8

**Exim attack**

- **BADSOC (n=9)**: 1, 8, 2
- **GOODSOC (n=17)**: 4, 14, 3
The attack trace library (AC-1) is depicted in (A). Attacks are generated (AC-2) by adding attack traces to the timetable (B), optionally changing playback speed and IP address rewriting (C). The attack injection (AC-3) is controlled using simple buttons. A red marker indicates the progress on the timeline (B).
More of SAIBERSOC...

- Try-it-yourself VM
- A (swagger) API
- Source Code
- Documentation
- User Manual
- Known Bugs
- ...

In the artifact repository

https://gitlab.tue.nl/saibersoc
Closing

Questions?
m.j.rosso@tue.nl

Additional material:
https://gitlab.tue.nl/saibersoc

Image: Luca Allodi @securescientist
https://twitter.com/securescientist/status/1205082605185589249