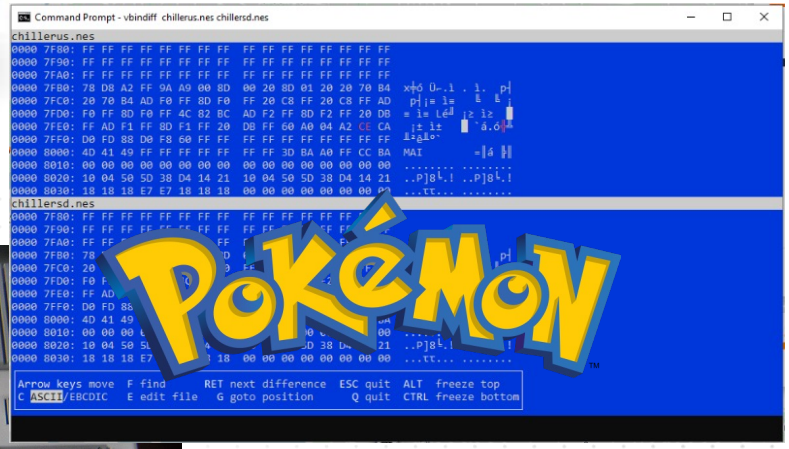
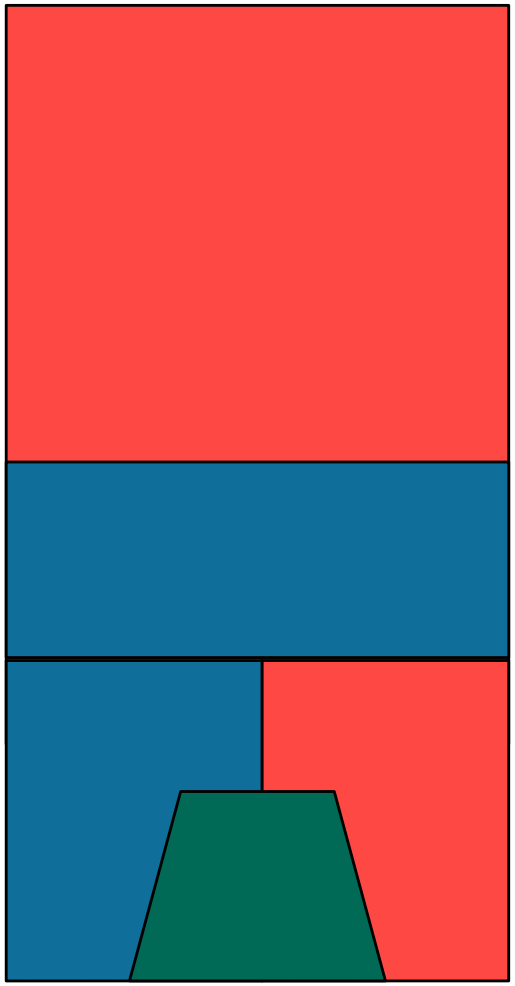

TL;DR
THREAT LED DIGITAL RED TEAMING
OFFENSIVE X
OUTFLANK
clear advice with a hacker mindset

WHOAMI


Command Prompt - vbindiff chillerus.nes chillersd.nes
chillerus.nes
chillersd.nes
Arrow keys move F find RET next difference ESC quit ALT freeze top
C ASCII/EBCDIC E edit file G goto position Q quit CTRL freeze bottom


Office



WHOAMI

OUTFLANK

FORTRA™

Outflank Security Tooling

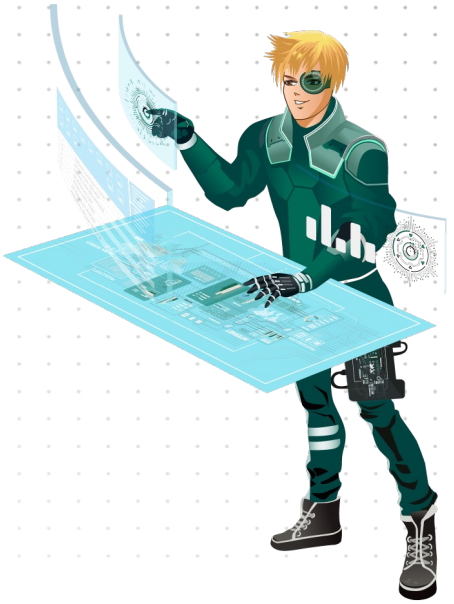
Tools and Tradecraft for Red Teams

Core Security

Penetration Testing Software
and Security Consulting Services

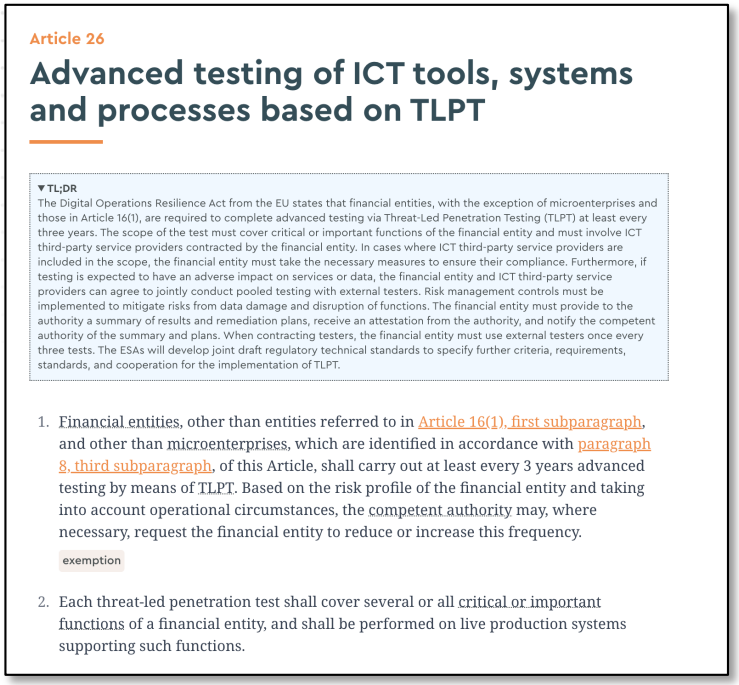
Cobalt Strike

Adversary Simulations
and Red Team Operations



LETS GO EXPLORING!

LEGAL TEXTS & STANDARDS



Article 26

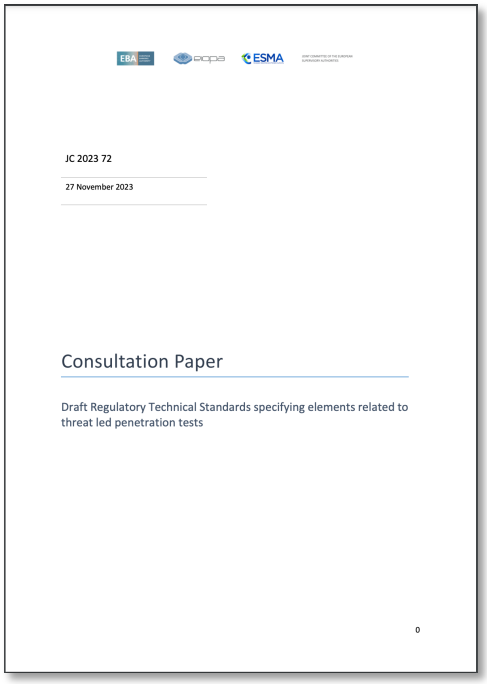
Advanced testing of ICT tools, systems and processes based on TLPT

▼ TL;DR
The Digital Operations Resilience Act from the EU states that financial entities, with the exception of microenterprises and those in Article 16(1), are required to complete advanced testing via Threat-Led Penetration Testing (TLPT) at least every three years. The scope of the test must cover critical or important functions of the financial entity and must involve ICT third-party service providers contracted by the financial entity. In cases where ICT third-party service providers are included in the scope, the financial entity must take the necessary measures to ensure their compliance. Furthermore, if testing is expected to have an adverse impact on services or data, the financial entity and ICT third-party service providers can agree to jointly conduct pooled testing with external testers. Risk management controls must be implemented to mitigate risks from data damage and disruption of functions. The financial entity must provide to the authority a summary of results and remediation plans, receive an attestation from the authority, and notify the competent authority of the summary and plans. When contracting testers, the financial entity must use external testers once every three tests. The ESAs will develop joint draft regulatory technical standards to specify further criteria, requirements, standards, and cooperation for the implementation of TLPT.

1. Financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, which are identified in accordance with paragraph 8, third subparagraph, of this Article, shall carry out at least every 3 years advanced testing by means of TLPT. Based on the risk profile of the financial entity and taking into account operational circumstances, the competent authority may, where necessary, request the financial entity to reduce or increase this frequency.

   exemption

2. Each threat-led penetration test shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions.



EBA ESMA

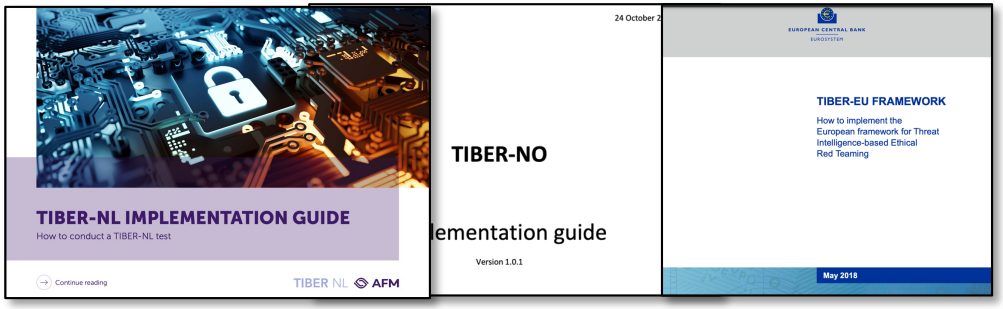
JC 2023 72

27 November 2023

Consultation Paper

Draft Regulatory Technical Standards specifying elements related to threat led penetration tests

0



TIBER-NL IMPLEMENTATION GUIDE
How to conduct a TIBER-NL test
Continue reading
TIBER NL AFM

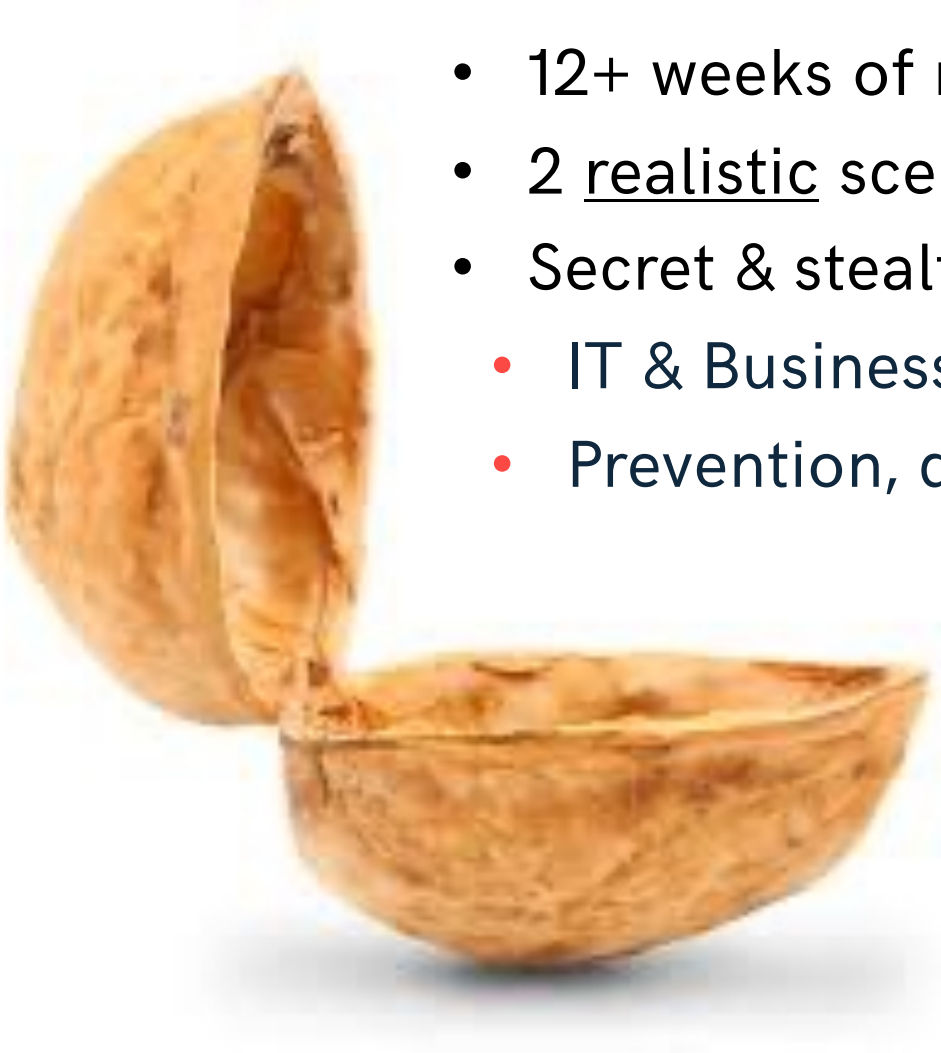
TIBER-NO
lementation guide
Version 1.0.1

EUROPEAN CENTRAL BANK
EUROSYSTEM
TIBER-EU FRAMEWORK
How to implement the European framework for Threat Intelligence-based Ethical Red Teaming
May 2018

- https://www.dora-info.eu/dora/article-26/#r11/
- https://www.esma.europa.eu/document/consultation-paper-draft-rts-tlpt

TL;DR
Per jan 2025:
If financial institution is ‘large’, then mandate threat led pen test

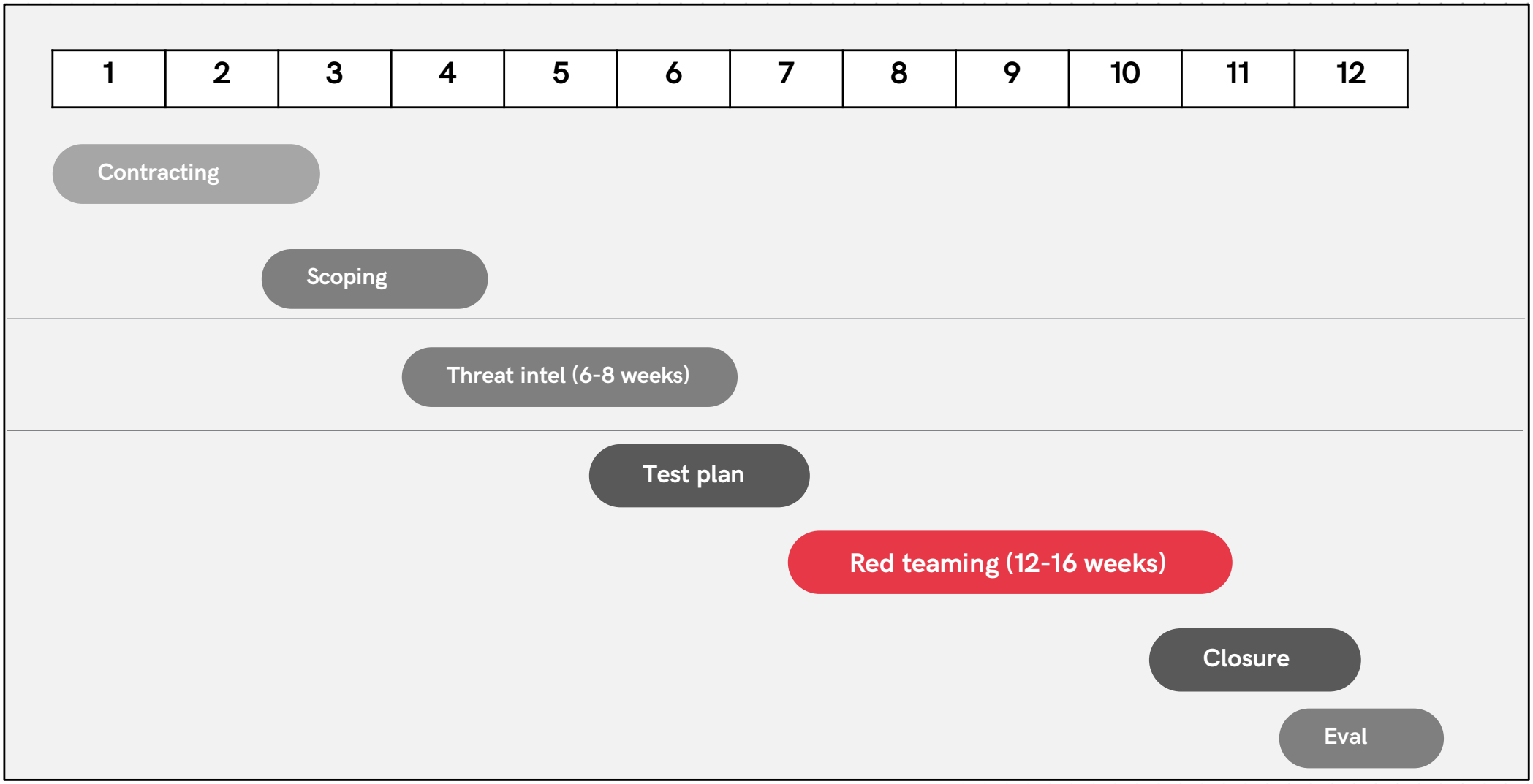
WHAT IS TIBER/DORA TESTING



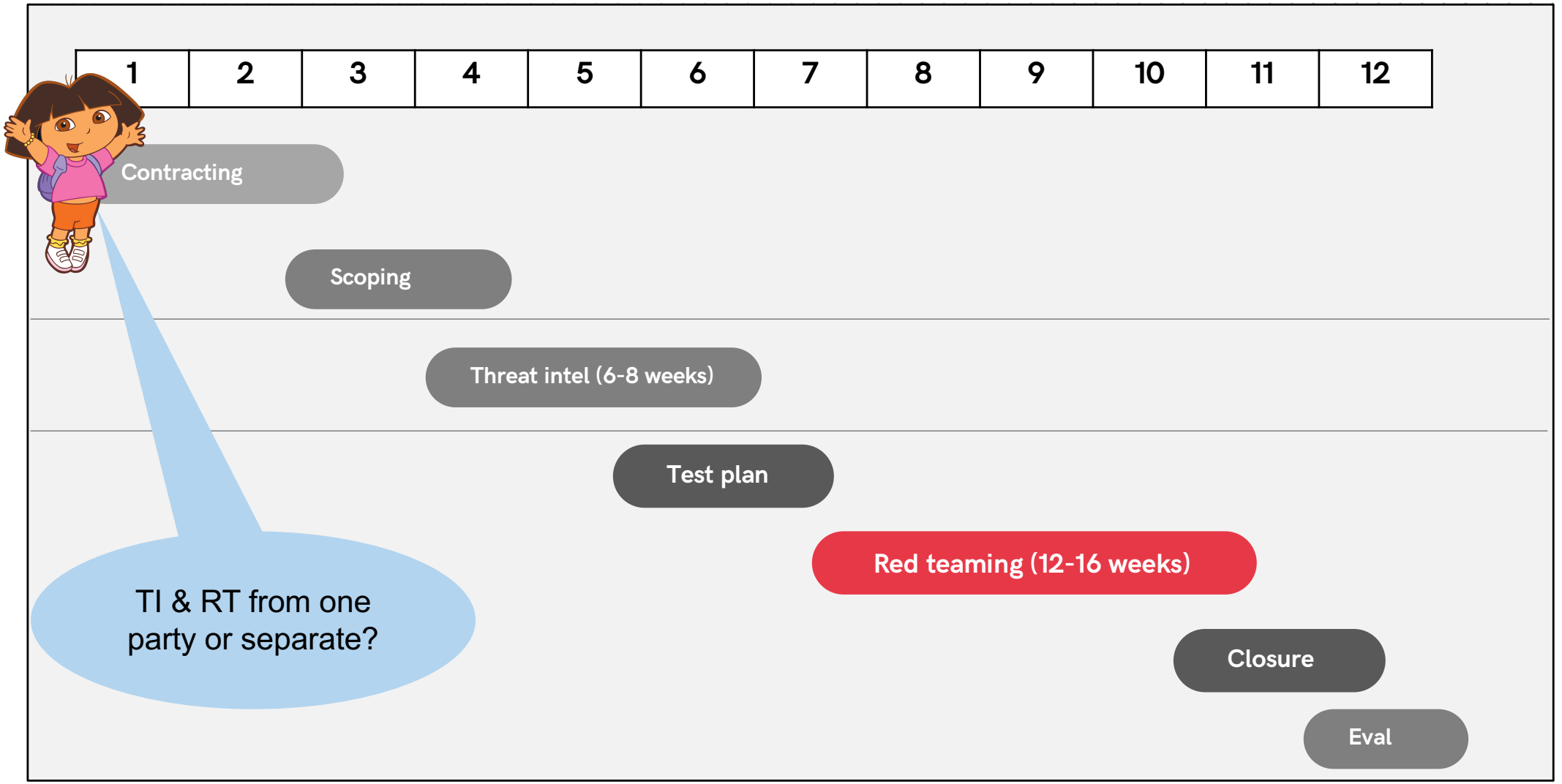
- 12+ weeks of red teaming (not fulltime)
- 2 realistic scenarios - end2end + 1 creative
- Secret & stealth execution
  - IT & Business controls
  - Prevention, detection & response

WHO'S WHO

ONE YEAR OF RED TEAMING



ONE YEAR OF RED TEAMING



ONE YEAR OF RED TEAMING

1	2	3	4	5	6	7	8	9	10	11	12

Contracting

Scoping

Threat intel (6-8 weeks)

Test plan

Red teaming (12-16 weeks)

Closure

Eval

ONE YEAR OF RED TEAMING

1	2	3	4	5	6	7	8	9	10	11	12

Contracting

Scoping

Threat intel (6-8 weeks)

Test plan

Red teaming (12-16 weeks)

Closure

Eval

What is this
'threat intel'?


THREAT INTEL
WIZARDRY
OUTFLANK
clear advice with a hacker mindset

THREAT INTEL

Goal:

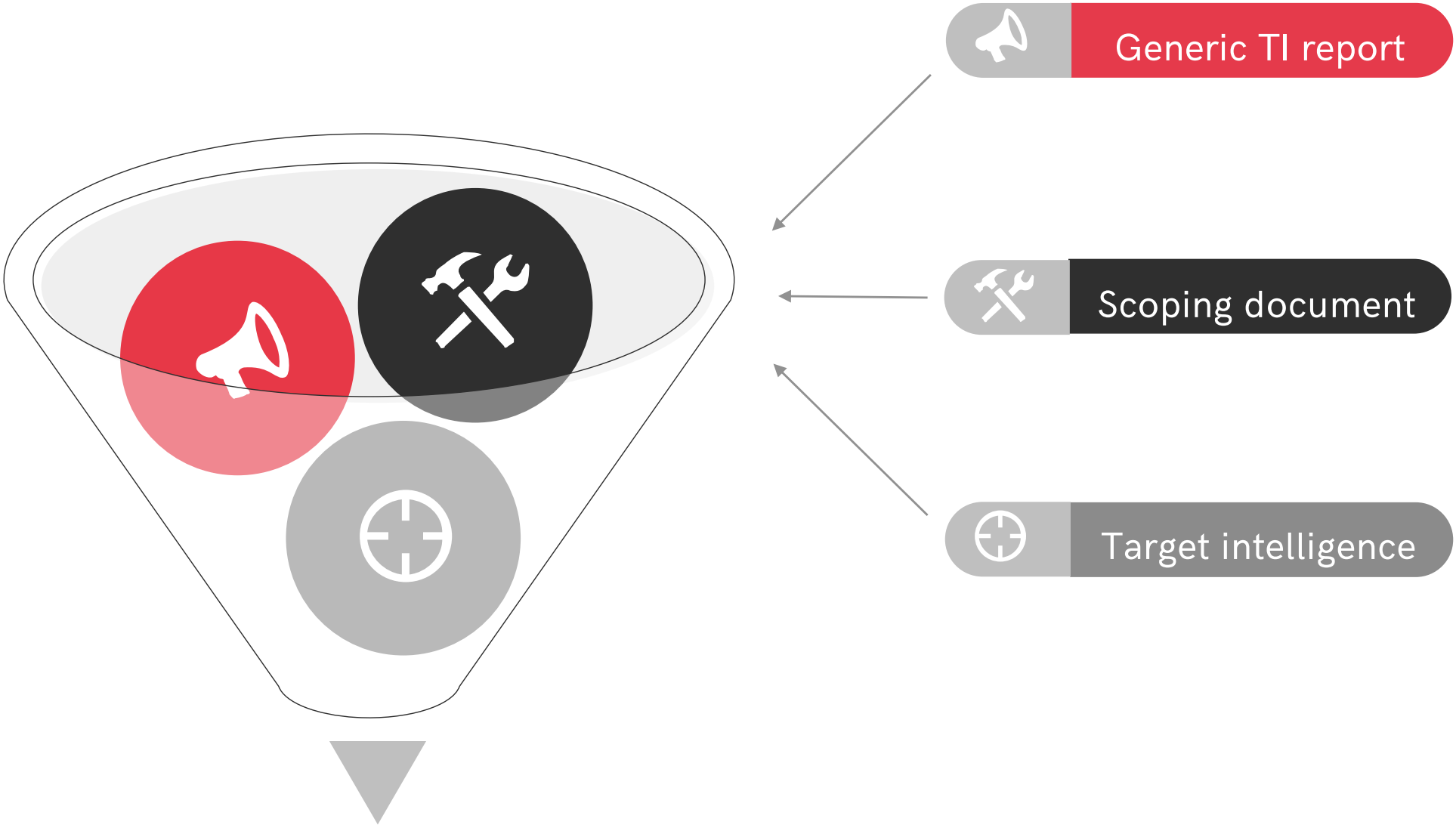
- provide scenarios for the red team to execute
- “passive” OSINT as input for RT

The suffering…

Some vendors

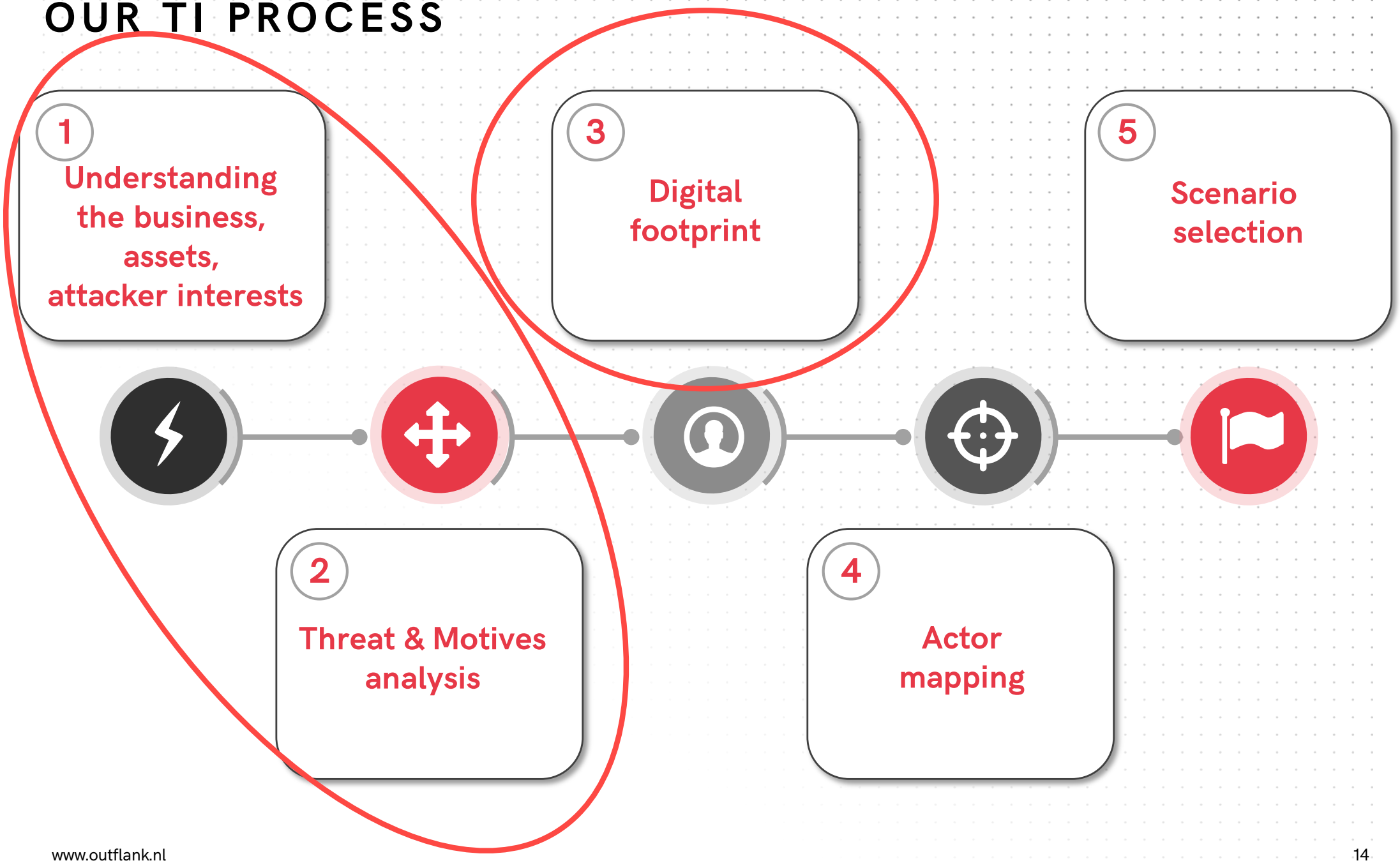
- Are making scenario building overly complex..
- Struggled with it, and centralized it around a list of MD5’s…
- Reported an extensive, non-actionable OSINT overview…

TI INPUT FOR SCENARIO SELECTION



2 scenarios based on current threats

OUR TI PROCESS



TI RESULTS

One scenario is always Ransomware

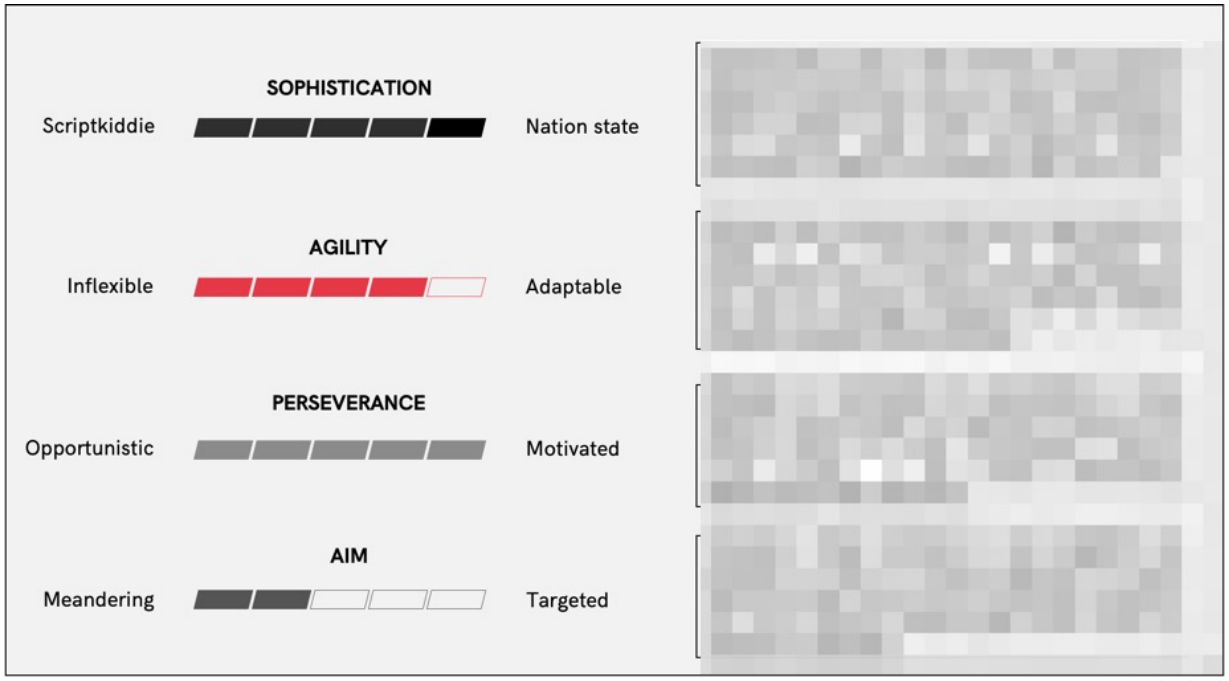
Scenario 2 depends on analysis & context:

genesis

Under the TIBER-BE national implementation, the TI provider is encouraged to include a physical breach scenario.

SCENARIO DESCRIPTION

- Narrative
- In-phase
- Out-phase
- Actor profile



ONE YEAR OF RED TEAMING

1	2	3	4	5	6	7	8	9	10	11	12

Contracting

Scoping

Threat intel (6-8 weeks)

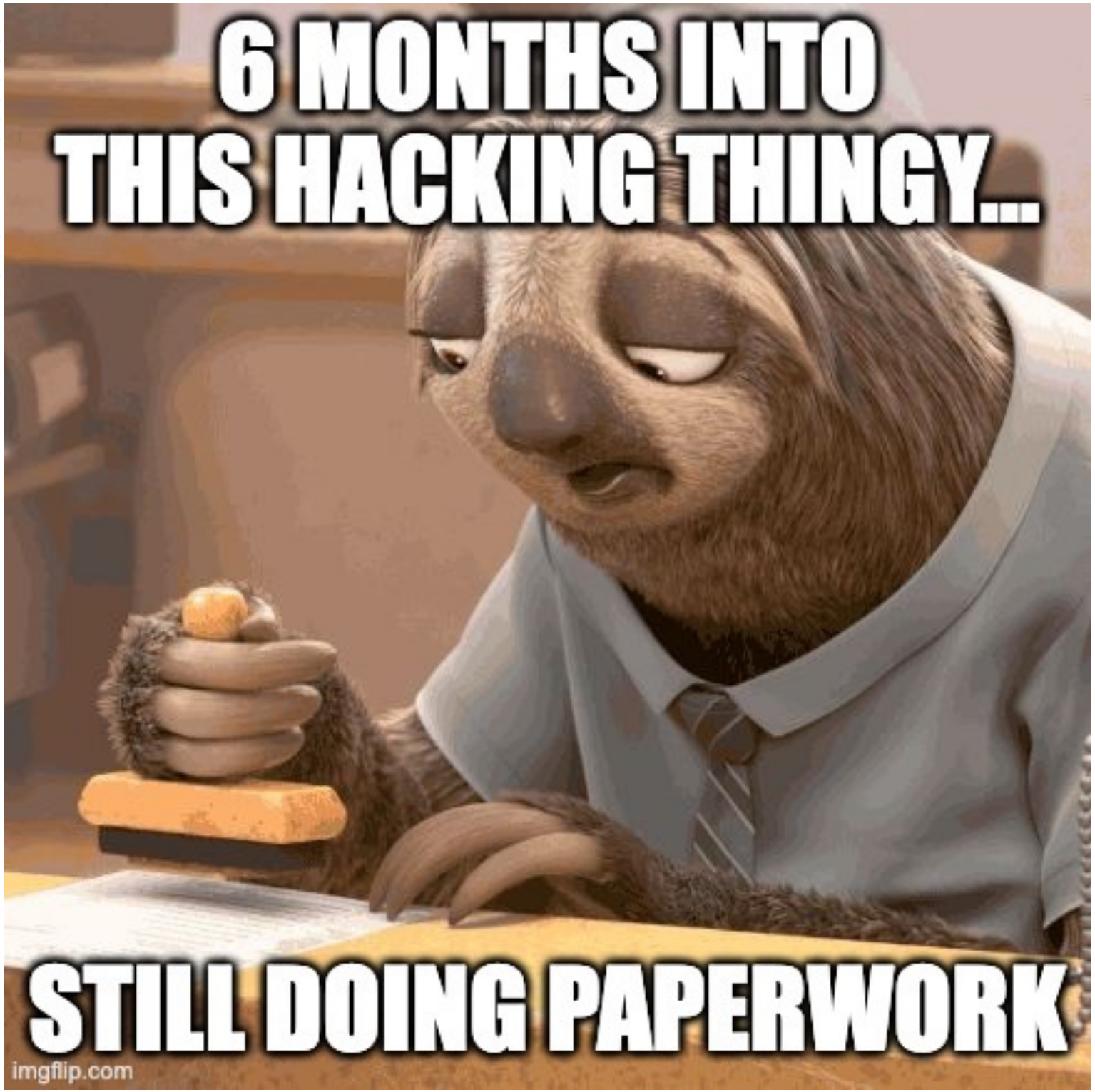
Test plan

The red team starts!

Red teaming (12-16 weeks)

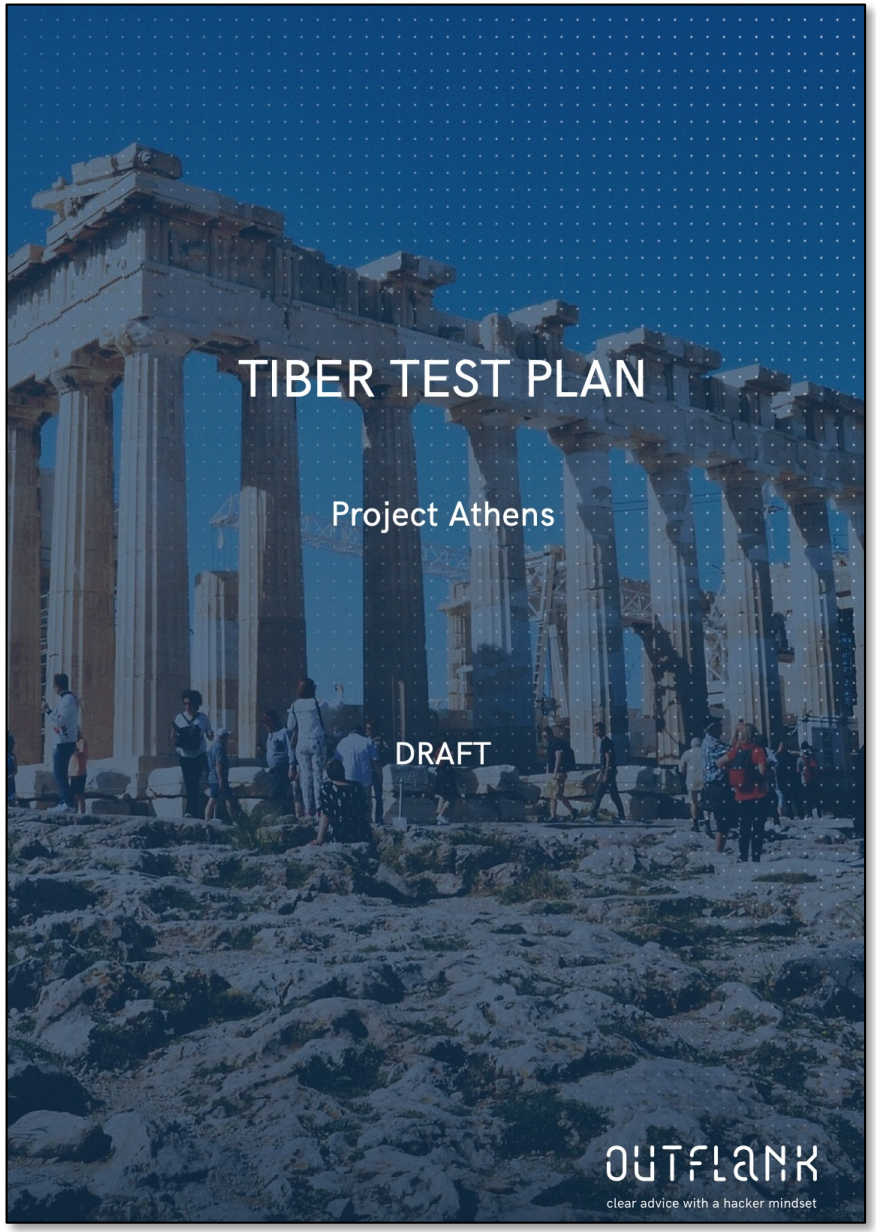
Closure

Eval


6 MONTHS INTO
THIS HACKING THINGY...
STILL DOING PAPERWORK
imgflip.com

TESTPLAN

- Organization
  - Communication processses
- Scenarios, milestones and planning
- Safety, privacy & risks
- Incident lifecycle:
  appetite and escalation?



ONE YEAR OF RED TEAMING

1	2	3	4	5	6	7	8	9	10	11	12

Contracting

Scoping

Threat intel (6-8 weeks)

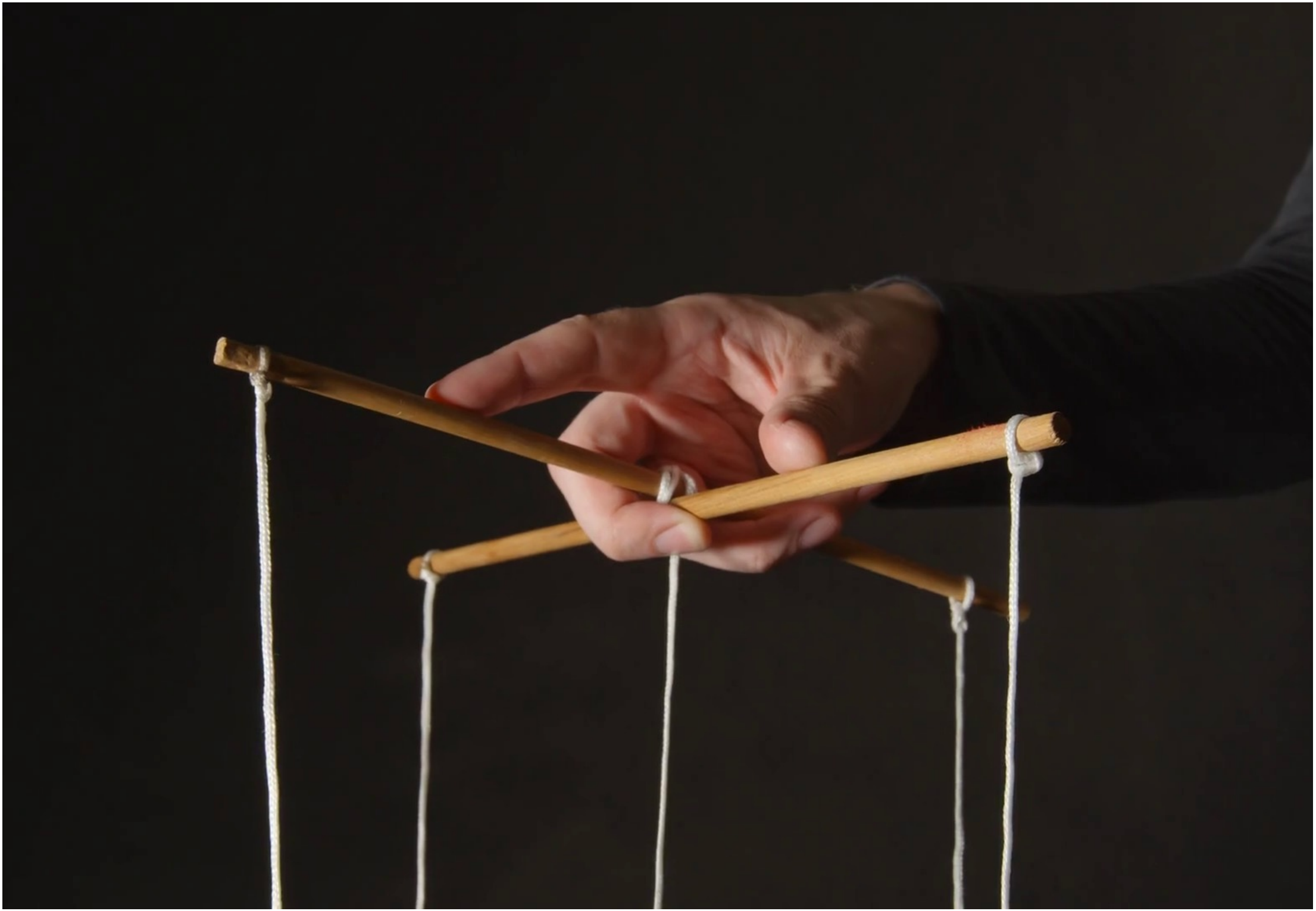
Test plan

Red teaming (12-16 weeks)

Finally, the hacking starts!

Closure

Eval



INFRA & PHISH

Opsec!

More sophisticated then real ransomware

Clickonce
Msc
Cloud attacks
…

AD HOC CAPABILITY DEVELOPMENT

- Time consuming
- “Latency”
- QA / opsec checks

```
#include "Klist.h"
#include "beacon.h"

#define MAX_MSG_SIZE 256
#define SEC_SUCCESS(Status) ((Status) >= 0)

INT iGarbage = 1;
LPSTREAM lpStream = (LPSTREAM)1;

HRESULT BeaconPrintToStreamW(_In_z_ LPCWSTR lpwFormat, ...) {
        HRESULT hr = S_OK;
        va_list argList;
        WCHAR chBuffer[1024];
        DWORD dwWritten = 0;

        if (lpStream <= (LPSTREAM)1) {
                hr = OLE32$CreateStreamOnHGlobal(NULL, TRUE, &lpStream);
                if (FAILED(hr)) {
                        return hr;
                }
        }
```

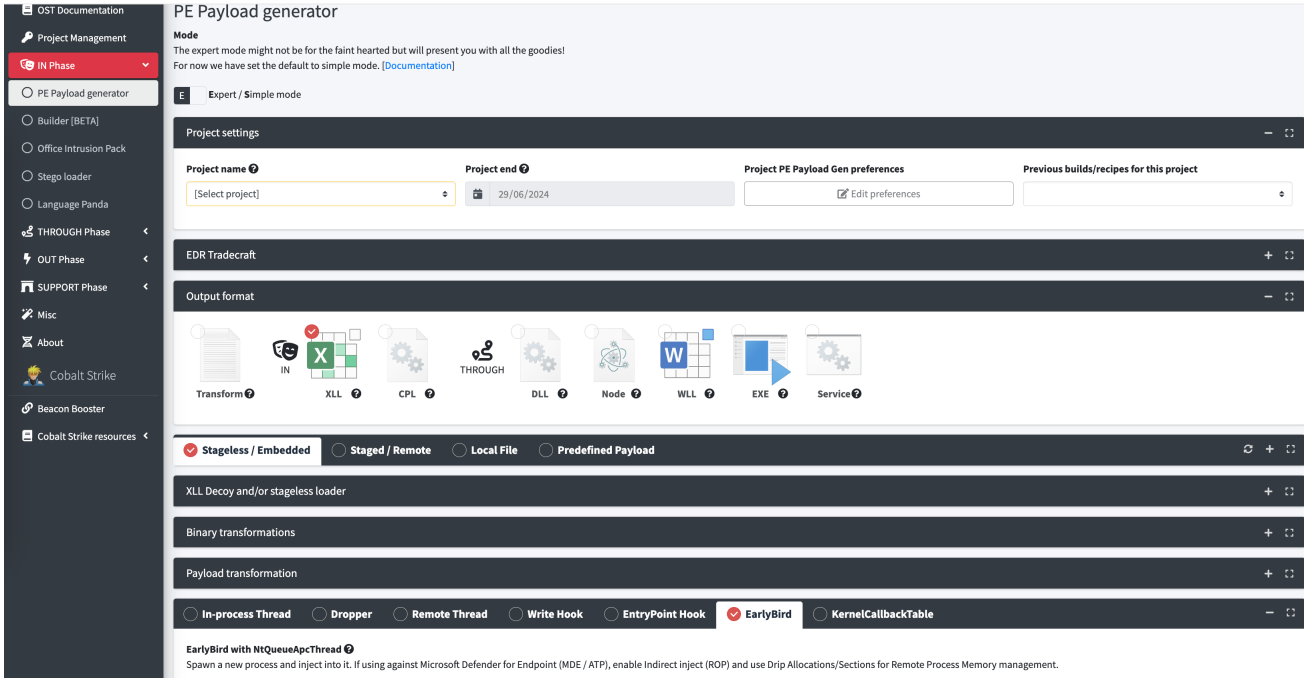
CAPABILITIES

Tools & development

- Evade any EDR/AV product
- ‘Ransomware as a service’
- Mimicking sophisticated actors,
  - Custom tools vs well-known tools
  - BYOVD
  - Credential stealers
  - .net obfuscator
  - Cloud attacks
  - …

MATURING

- Spending lots more time, maturing tools
- Developing capabilities we initially not really needed/used



How to structure & fund offensive R&D for those tests?

LEG UPS

WEEK 6 - SCENARIO 3/X

Forward looking/creative

Can be stacked on top of 1 or 2

- Other actions on objectives

Not perse TI driven

- Target something ‘different’
  Business dept/dev env/...
- Non-tech (e.g. deepfakes & CEO fraud)
- Simulate more complex attack paths

(e.g. supply chain towards other orgs)

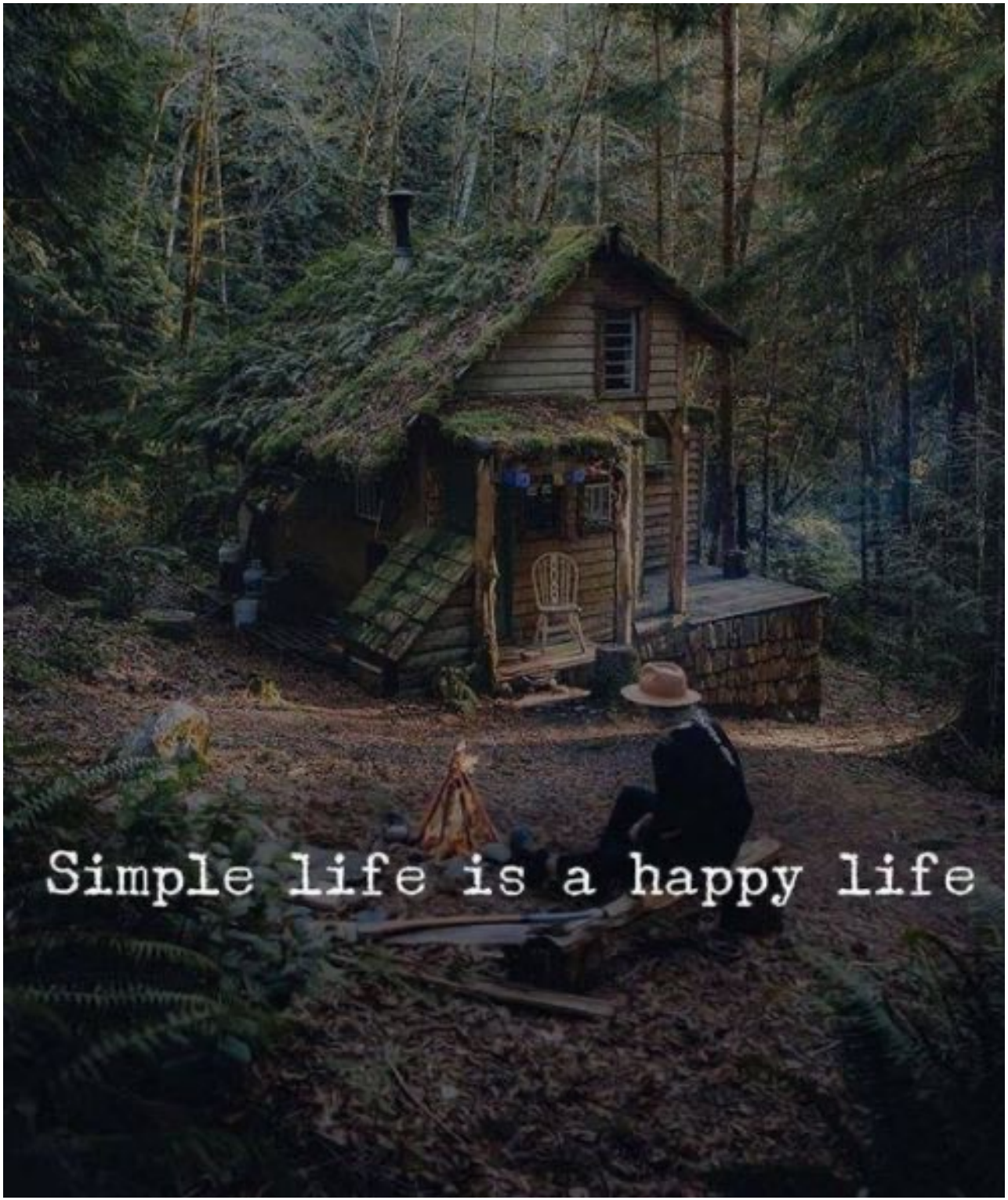

THIS ONE TIME..
AT BAND CAMP

THE SIMPLE LIFE

One time at Red teaming…

Lesson learned:

"try harder" is not always the solution



THE ONE WITH THE MONEY

One time at Red teaming

- Got access to core banking systems
- Transferred $$

- Days later white team calls….
  - the money was gone, but not received on the target bank account
  - Regular org / blue did not noticed the theft yet

Lesson learned: Risk management

ONE YEAR OF RED TEAMING

1	2	3	4	5	6	7	8	9	10	11	12

Contracting

Scoping

Threat intel (6-8 weeks)

Test plan

Red teaming (12-16 weeks)

Closure

Eval

CLOSURE

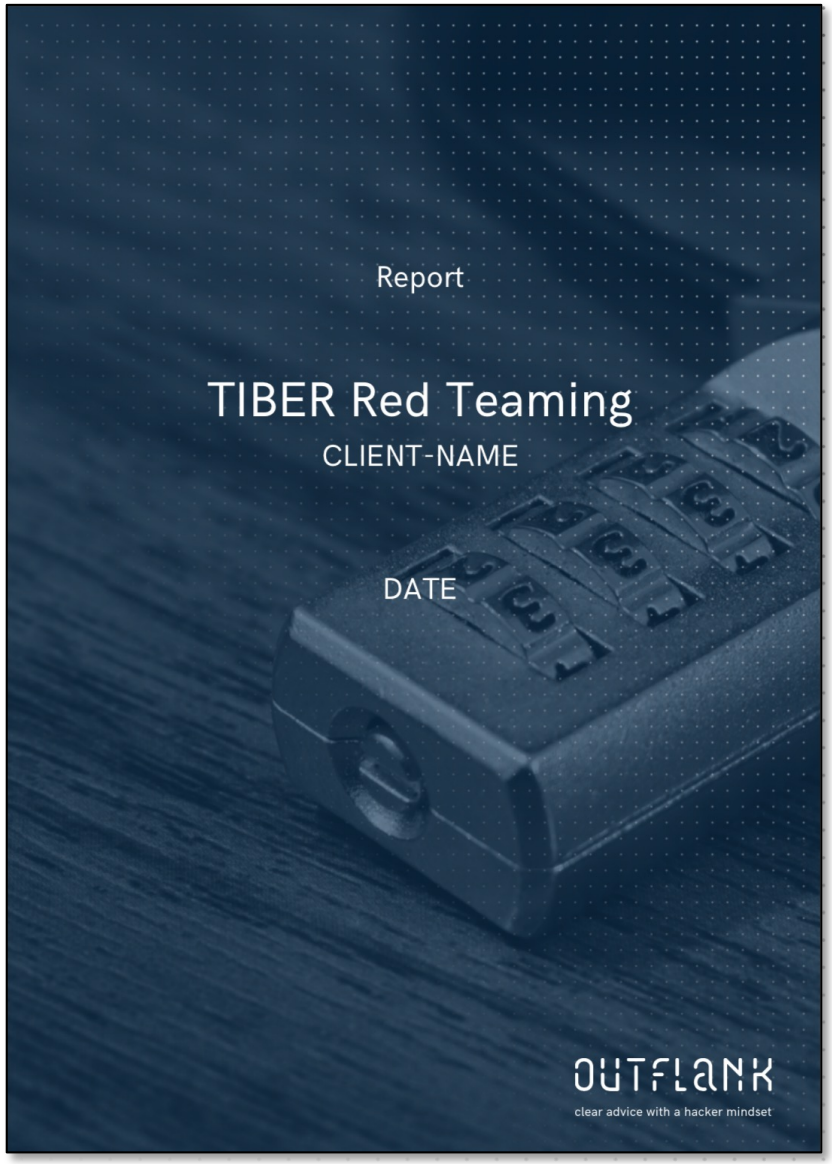
Reporting

Replay / purple

- Care for Emotions
- Blue team first!

After test completion

- White/blue team: Mitigation plan



METRICS EXPERIMENTS

	Time to **objective**	Time to **investigation**	Time to **recovery**	Total period of **access**
Scenario 1	XX days	XX Not detected	X Not recovered	YY+ Days
Scenario 2	XX days	X days	Y Not recovered	ZZ days

TIBER METRICS	
RECON	
Online exposure	
IN	
User behavior	
Workstation security	
THROUGH	
Server & network security	
Authorization management	

ONE YEAR OF RED TEAMING

1	2	3	4	5	6	7	8	9	10	11	12

Contracting

Scoping

Threat intel (6-8 weeks)

Test plan

Red teaming (12-16 weeks)

Eval


TOO LONG DIDN'T LISTEN
OUTFLANK
clear advice with a hacker mindset

DORA CAN BE FUN!

Organize yourself

- More engagement management, politics and all
- Inhouse TI?
- Proper opsec & evasion challenges
- Professionalize capability development / R&D

The fun

- Higher budget, longer test period,
- Really making business impact, activating detection etc
- Stronger drive for change after test

The market

- Other companies ask ‘similar’ test; even more fun!

+31 6 5157 2696
pieter@outflank.nl
www.outflank.nl/pieter

OUTFLANK

clear advice with a hacker mindset

+31 6 5157 2696
pieter@outflank.nl
www.outflank.nl/pieter

OUTFLANK

clear advice with a hacker mindset