

The background is a blue-tinted aerial map of a landscape with numerous winding, irregular lines representing trenches or ditches. Some of these lines are labeled with handwritten-style text: 'COMMUNITY TRENCH', 'DEFENCE', 'DUG-OUTS', and 'T-OUTS'.

TALES FROM THE TRENCHES

THE GOOD, BAD & UGLY
OF 6 YEARS THREAT
INTELLIGENCE IN TIBER

CYBER RESILIENCE DAY

CM.COM & OUTPOST24

ORDER OF BATTLE

LENNERT BRANDERHORST

TI LEAD AT TIBER-NL



L.J.BRANDERHORST@DNB.NL



A little history: TIBER-NL & Threat Intelligence



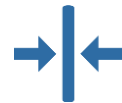
The good



The bad



& The ugly



Aligning vendor & customer

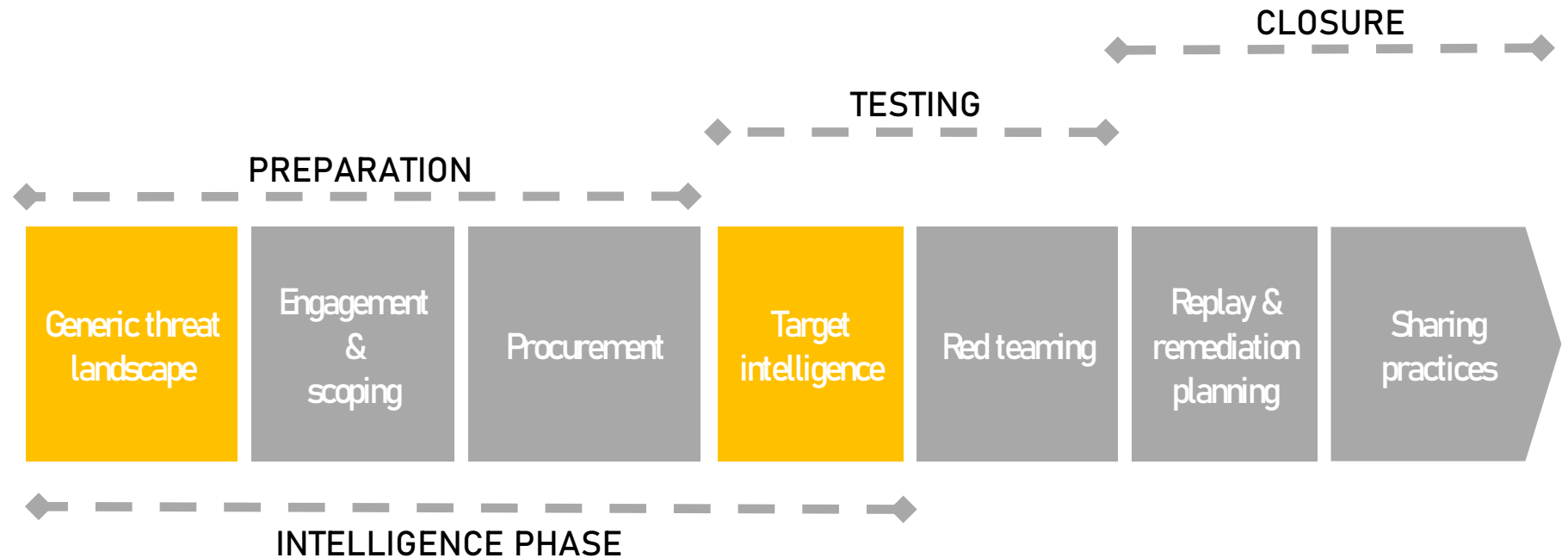
TIBER-NL & THREAT INTELLIGENCE



40+ TIBER-tests through multiple sectors & countries.



Added value recognised by participating institutions.



THE GOOD THE BAD AND THE UGLY

AFTER 6 YEARS OF
THREAT INTELLIGENCE
IN TIBER-NL TESTS

WHAT WENT WELL?

WHAT DID NOT?

WHAT ARE SOME 'UGLY' TRUTHS?

THE GOOD

AFTER 6 YEARS OF
THREAT INTELLIGENCE
IN TIBER-NL TESTS



CARTE
BLANCHE

TIBER enabled TI and RT-providers to come up & carry out scenarios that were not possible until then.



TUNNEL
VISION

External TI helps to prevent tunnel vision in internal red teams. A fresh perspective really helps.



MONEY

An institution can build its cyber defenses more cost-efficient if it knows whom it's up against.



THE BAD

AFTER 6 YEARS OF
THREAT INTELLIGENCE
IN TIBER-NL TESTS



SO NOW
WHAT?

It is hard to make TI actionable & useful. This is due to both the TI provider and receiving organisation.



GROUNDHOG
DAY

In recurring tests, TI can become a bit repetitive and add (too) little extra value for the customer.



BLABLA
BLABLA

Longer doesn't always mean better. TI-reports are often too lengthy to get the main point across.

AND THE UGLY

AFTER 6 YEARS OF
THREAT INTELLIGENCE
IN TIBER-NL TESTS



LEMON MARKET PART 1

The market for TI-providers is not transparent. Big differences between and within companies.



LEMON MARKET PART 2

Quite often, the customer / institution is not able to process TI due to own restrictions and limitations.



MIS MATCH

Because of this, there is often a mismatch between what a customer expects and what a provider delivers.

Aligning vendor & customer



ART
(ADVANCED RED TEAMING)

Different Red Teaming frameworks to fit different needs.



**MANAGING
EXPECTATIONS**

If you start with a TI function in your company from scratch, adjust your expectations. Know yourself.



KYC
(KNOW YOUR CUSTOMER)

Know your customer. Be prepared to have an honest discussion on what he wants and what you can deliver.

QUESTIONS

