TLP:CLEAR

From TTPs to Deception: Crafting Strategies

Diego Staino
R&D+i Manager

Federico Pacheco
Cybersecurity Services Director

BASE4
SECURITY

About us

Diego Staino

R&D+i Manager

14+ years of consulting experience

Bachelor in Information Security

Federico Pacheco

Cybersecurity Services Director

20+ years of university teaching experience

4 published books | 15+ whitepapers

Our peer reviewed work

- "Active cyber defense: service model for defensive strategies based on the adversary's error" (Pacheco, 2022)
  - https://rtyc.utn.edu.ar/index.php/ajea/article/view/1146/1059
- "Proposal for the implementation of minimalistic cyber deception strategies" (Pacheco, Staino, 2024)
  - http://dx.doi.org/10.13140/RG.2.2.34289.29289
- "Reinforcement of cyber deception strategies through simulated user behavior" (Pacheco, Staino, 2025)
  - http://dx.doi.org/10.13140/RG.2.2.20886.87368

Cyber Deception 101

“In times of deception, telling the truth is a revolutionary act”

BASE4
SECURITY

Deception basics

* with offensive approach

* +detect or hinder

"Defensive practice that aims to deceive attackers through of traps and decoys in an infrastructure or system that mimic real assets."

*or they are real

*our

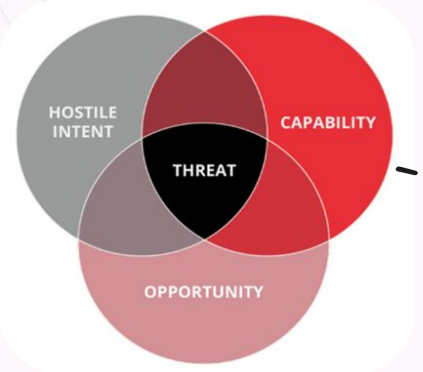
512 BC

MITRE | Engage™

2022

TTPs and Threat Intelligence 101

BASE4
SECURITY



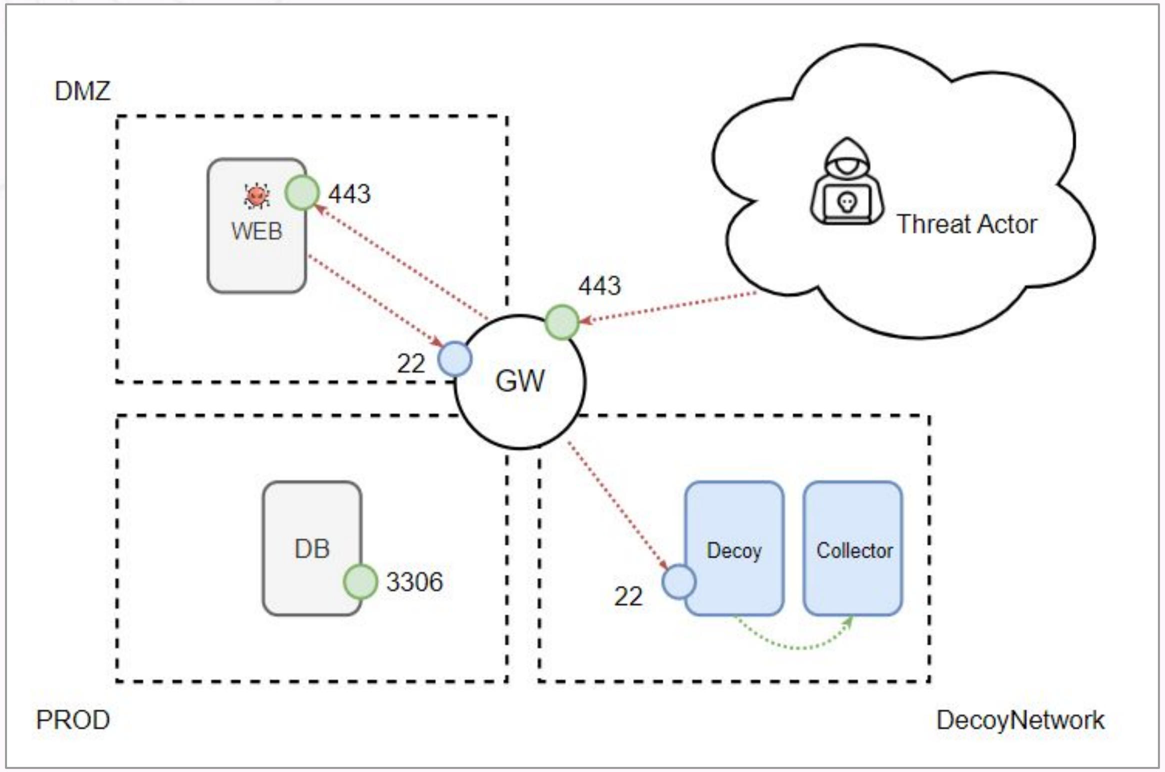
MITRE ATT&CK™

Cyber Threat Intelligence (CTI)

Actionable knowledge about adversaries and malicious activities, enabling defenders to reduce harm through better security decision-making

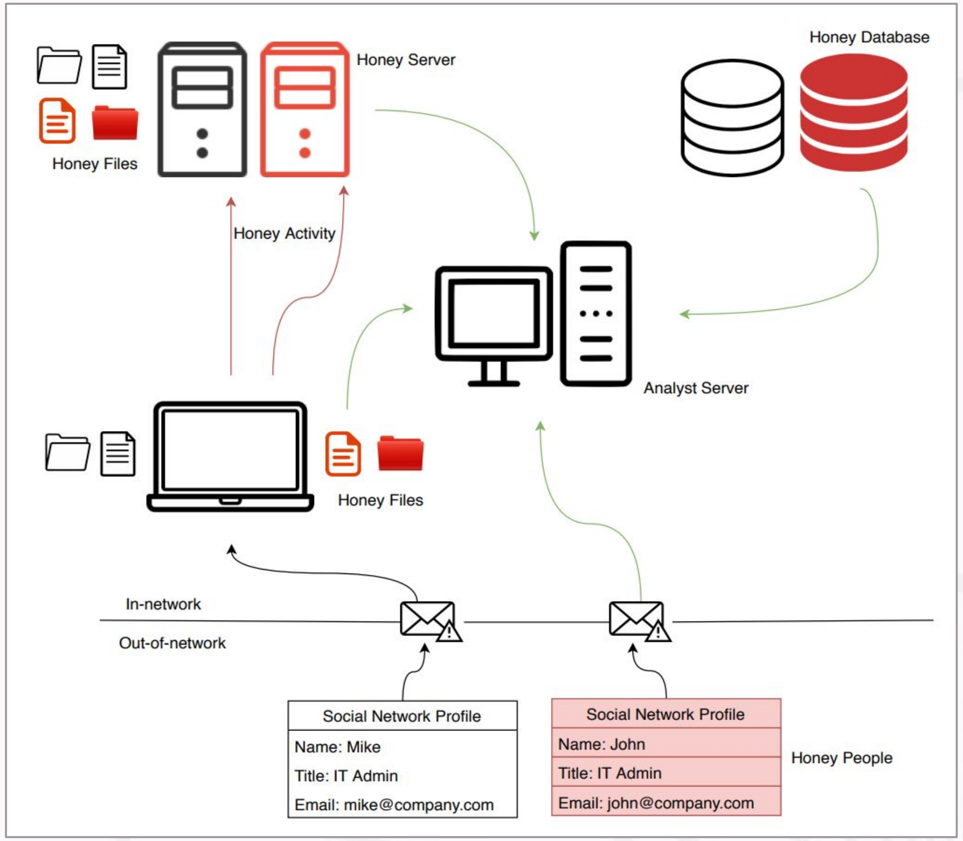
Let’s see some cases

BASE4 SECURITY



DOLOS Tool - Use Case for Web Server

Paper: “Proposal for the implementation of minimalistic cyber deception strategies” Pacheco, Staino, 2024



Social Network Profile
Name: Mike
Title: IT Admin
Email: mike@company.com

Social Network Profile
Name: John
Title: IT Admin
Email: john@company.com

Paper: “Detecting Targeted Attacks By Multilayer Deception” Wang et al, 2013

Context: Why a methodology?

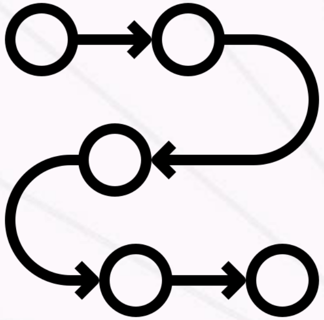
Case A want…

… no budget for solutions
… cannot take risks
… low experience on deception

Case B want…

… enhance available solutions
… to do more
… operationalize Deception

Keep it Simple Stupid



Behavior Extraction

“We don’t see things as they are, we see them as WE are”

Not all the observables are created equal

“XXX leverage DNS tunneling for data exfiltration”

“YYY use PowerShell to execute scripts”

“ZZZ use print processors to run malicious DLLs”

Indicator ≠ IoC ≠ Behavioral invariant ≠ TTP

Sources of CTI

BASE4 SECURITY

Log & Trace analysis

- Data correlation
- Sandboxing
- Look for Interesting activity

OSINT & CTI Platforms

OpenCTI | Maltego | Dark Web | …

VirusTotal | MISP | …

Reports from Govs & Orgs

MITRE ATT&CK | CISA | Europol EC3 | FIRST |

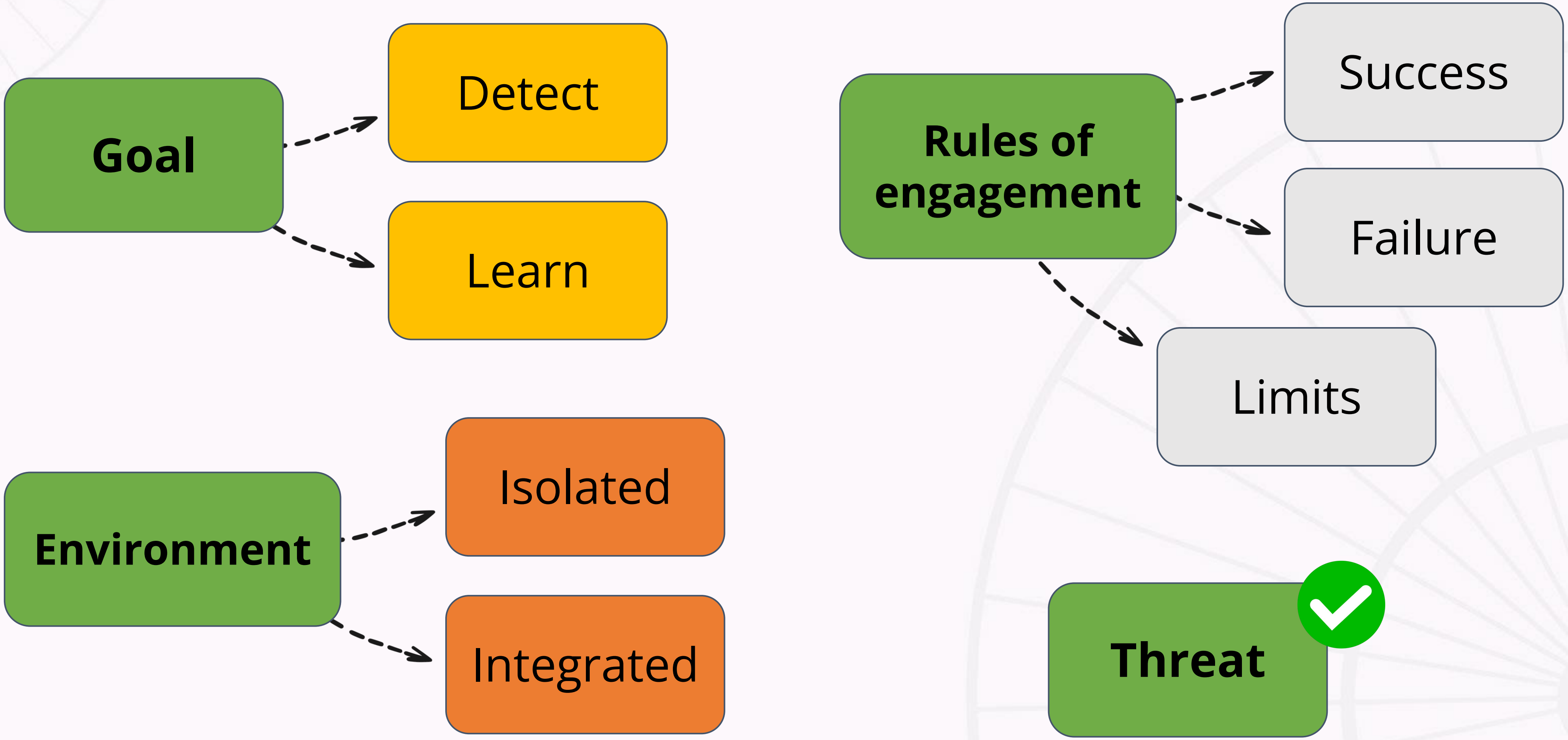
Mandiant | CrowdStrike | SentinelOne | Unit 42 | …

Criteria Selection

“A well-chosen lie is like a tailor-made suit: it fits perfectly for the occasion, even if it’s not made of truth.”

Base element selection

*minimum



Goal

Detect

Learn

Environment

Isolated

Integrated

Rules of engagement

Success

Failure

Limits

Threat ✓

Understanding Risk & Impact

What if …

… the adversary uses your env to distribute malware?

… a decoy user is detected using a prod service?

… a zero-day is exploited in the isolated env?

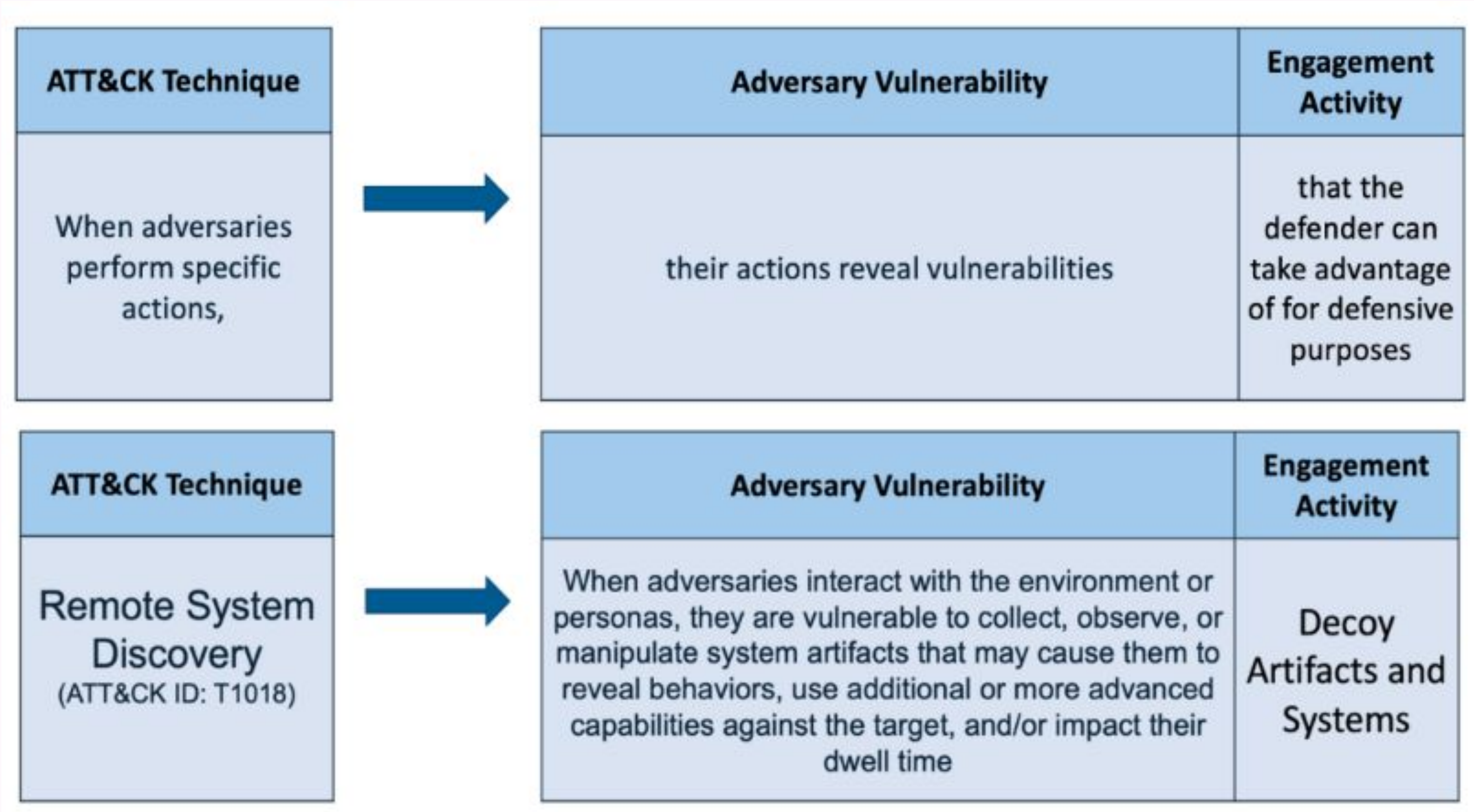
* Release your anxiety and ask questions *

Translation of TTPs into activities

"The art of persuasion lies in choosing your words with precision, whether you're constructing a truth or a lie."

Meta Quest
Meta Quest
KARMA
PAUL
VS
ROUN
NETFLI

The vulnerability of the attack



ATT&CK Technique	Adversary Vulnerability	Engagement Activity
When adversaries perform specific actions,	their actions reveal vulnerabilities	that the defender can take advantage of for defensive purposes

ATT&CK Technique	Adversary Vulnerability	Engagement Activity
Remote System Discovery (ATT&CK ID: T1018)	When adversaries interact with the environment or personas, they are vulnerable to collect, observe, or manipulate system artifacts that may cause them to reveal behaviors, use additional or more advanced capabilities against the target, and/or impact their dwell time	Decoy Artifacts and Systems

"A Practical Guide to Adversary Engagement" (MITRE Engage)

Examples of vulnerabilities behind attacks

MITRE TTP	Attacker Vulnerability	Detection Risk	Detection Examples
Cmd and Scripting Interpreter - T1059	Commands logged (e.g., PowerShell, Bash history)	Correlation of commands, script, execution path	PowerShell logs, Sysmon, Win Events (4104), EDR
Remote Services: RDP T1021.001	Session artifacts (Event IDs, IP addresses, login times)	Log correlation, session replays	Win Events (4624, 4778)
Signed Binary Proxy Execution - T1218	Abuse of known binaries creates behavioral patterns	Heuristic detection, parent-child process anomalies	Sysmon (ID 1) EDR rules
OS Credential Dumping T1003	Access to LSASS may trigger memory access alerts	Known tool signatures, volatile memory artifacts	Sysmon, Anti malware, mem dump
App Layer Protocol: Web-HTTP/S - T1071.001	C2 traffic can leak IOCs (domain, headers, JA3 fingerprint)	NDR inspection, beaconing patterns	Zeek, Suricata, Wireshark

Starting with Activities

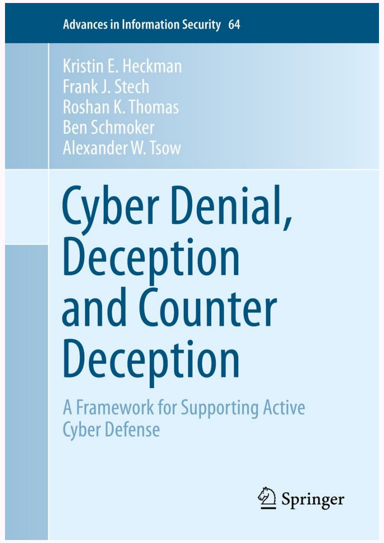
Goal

Rules of engagement

Deception Activity

+Ambiguity
(A-Type)

+Misleading
(M-Type)



Advances in Information Security 64

Kristin E. Heckman
Frank J. Stech
Roshan K. Thomas
Ben Schmoker
Alexander W. Tsow

Cyber Denial, Deception and Counter Deception

A Framework for Supporting Active Cyber Defense

Springer

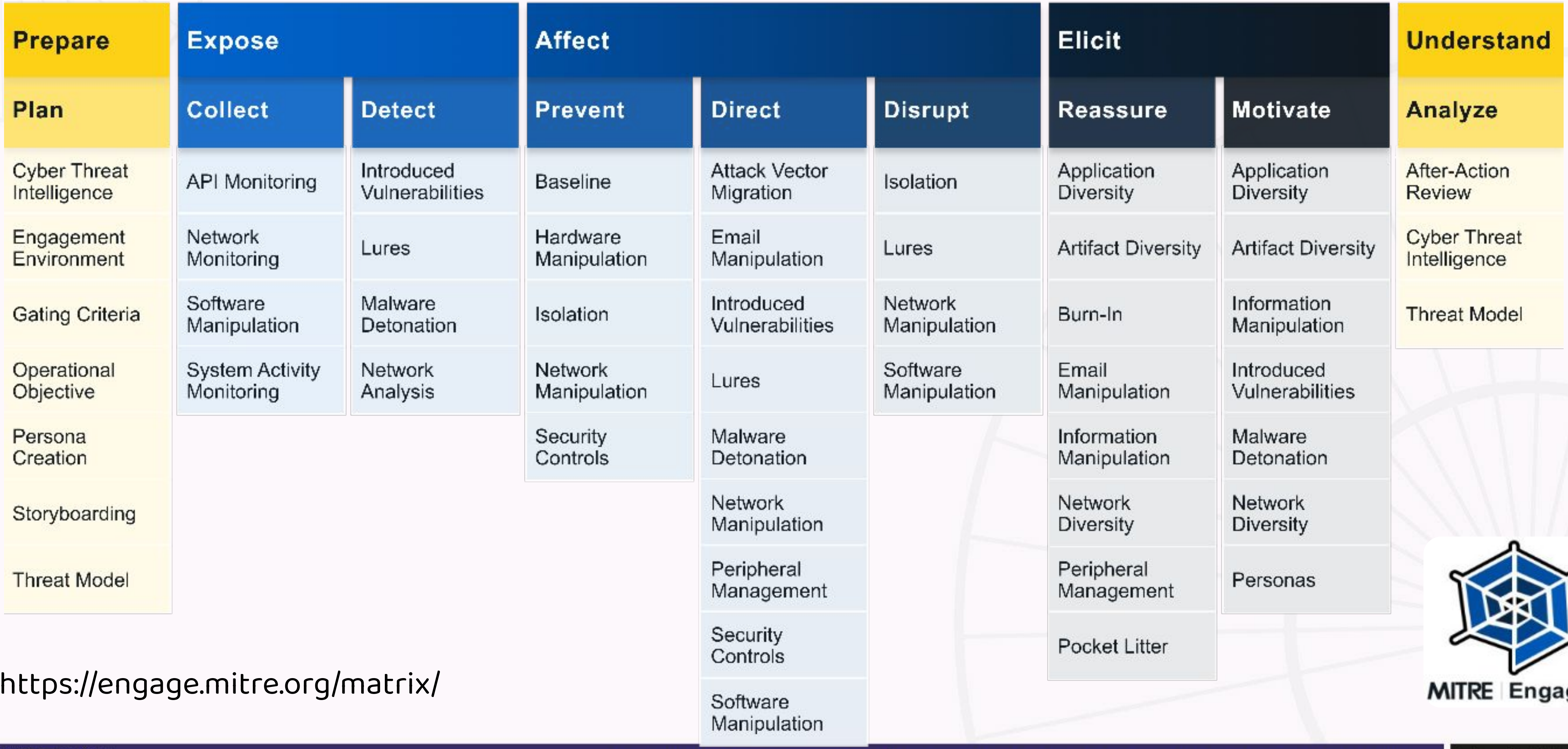
Expose

Affect

Elicit

MITRE | Engage™

MITRE Engage Matrix

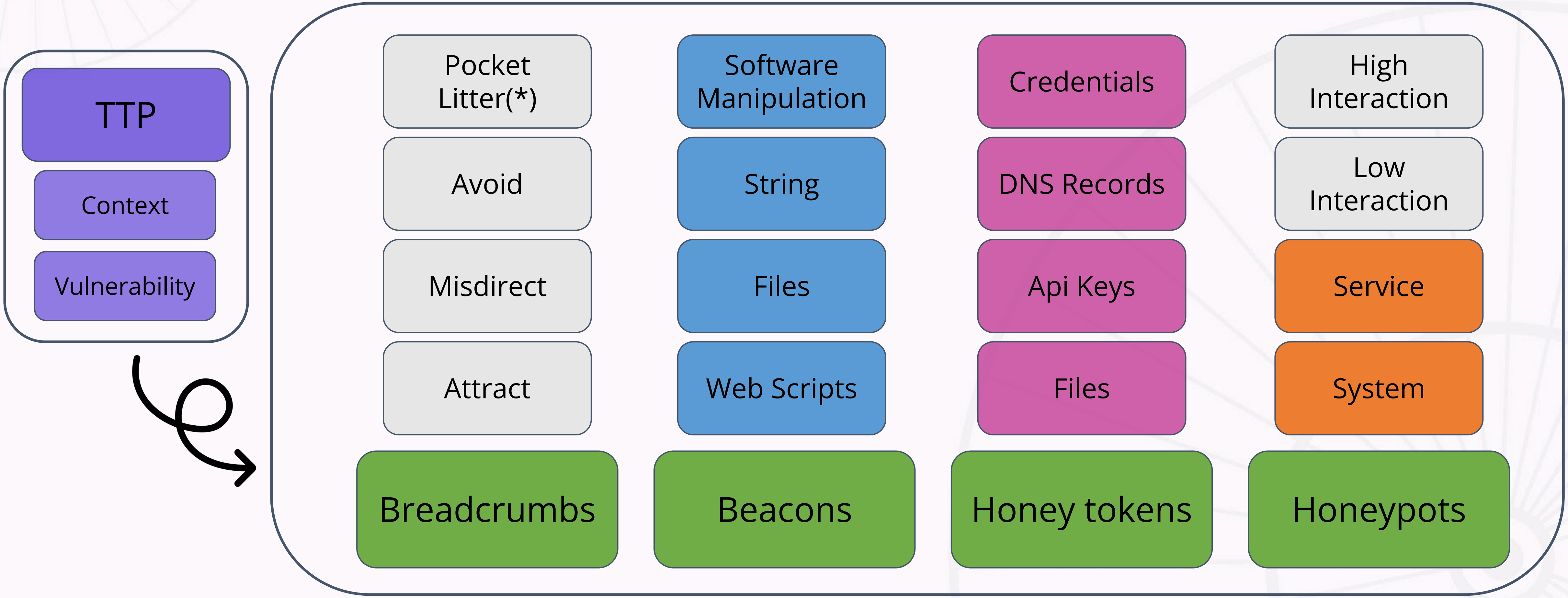


Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

https://engage.mitre.org/matrix/

MITRE | Engage™

Mapping TTPs to Activities



TTP

Context

Vulnerability

Breadcrumbs	Beacons	Honey tokens	Honeypots
Pocket Litter(*)	Software Manipulation	Credentials	High Interaction
Avoid	String	DNS Records	Low Interaction
Misdirect	Files	Api Keys	Service
Attract	Web Scripts	Files	System

A few tips

Just pick one and try it

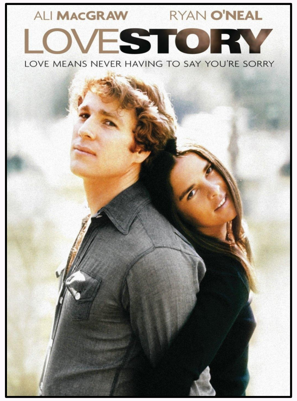
- It might be the most used TTP
- Mix creativity with reality
- Start thinking small
- Take care of the risks and the complexity

Storytelling Design

"Every good story begins with a lie that invites us to see the world in a different light."

It's all about the story

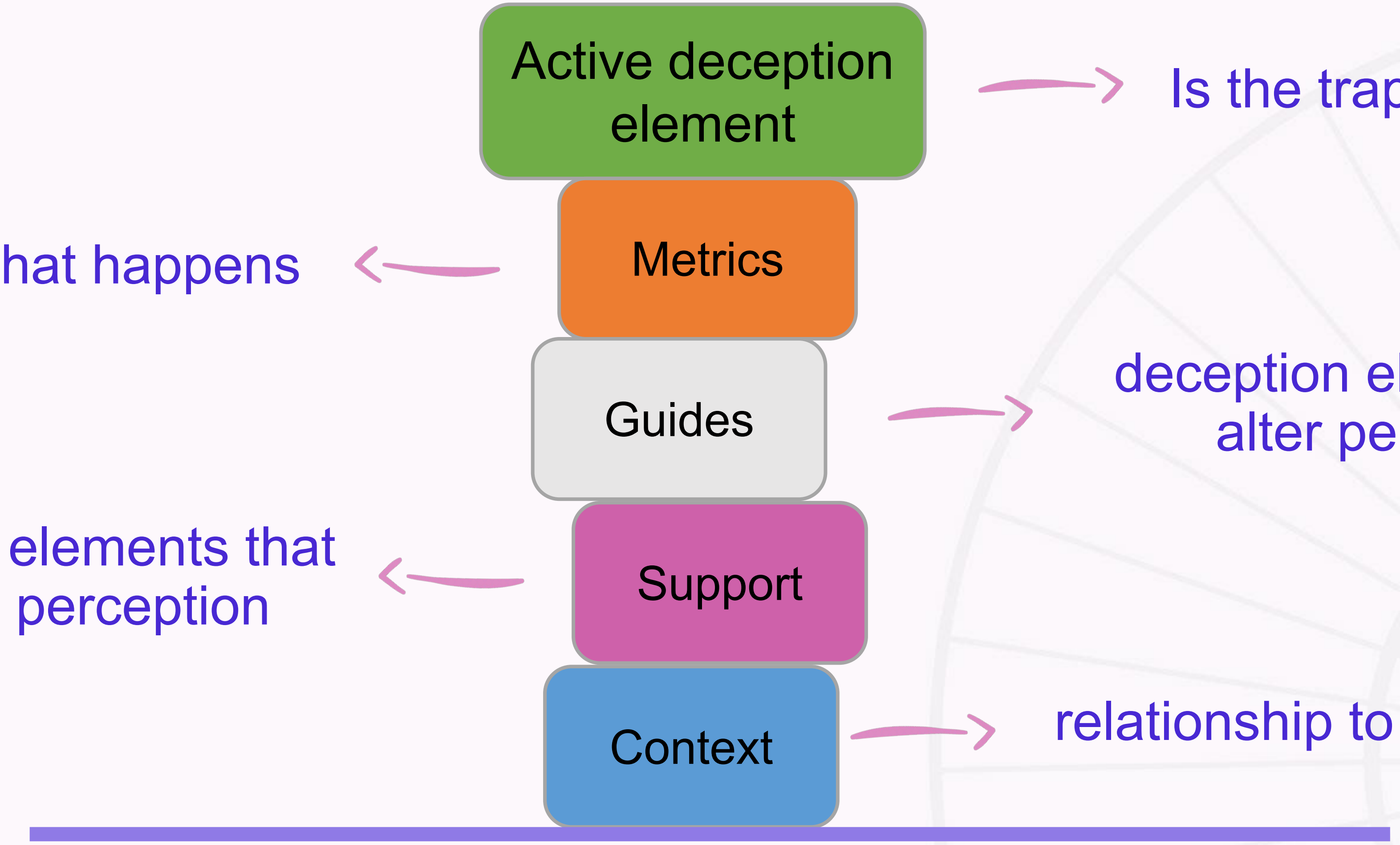
- Integral narrative (everything must make sense)
- Why is this service here?
- The narrative supports your deception
  (you deal with humans!)



Deception Strategy

Port 22 on Windows

Elements of a Story



Active deception element → Is the trap!

Metrics → collect what happens

Guides → deception elements that alter perception

Support → deception elements that confirm perception

Context → relationship to env elements

Some examples

A company dedicated to robotics and AI research

- Research notes and pseudo-code snippets in the Dev Team Workstastion that point to a QA web application.
- A DNS record and browser bookmarks for the same web application.

A global financial institution with a trading platform

- Fake user registered on intranet and core services.
- The user is a financial executive with a common name.
- Email credentials “self-leaked".
- The email account is created and registered in some financial social networks.

Questions?

CYBER-ATTACK
HACKERS
DENDIFENDERS
PROT TWISS
CREATIVE STORY
INTTELG
CYBERSCURITY
DECEPTI
DEFEN
DECEPSION
CREATIVE STORYT

Time to work

Your next steps

Short term:

- Read your notes and mentally analyze at least five different scenarios for using the deception strategies.

Middle term:

- Try to identify small opportunities to apply deception on your environment (sometimes small is enough).
- Start with zero risk activities.

Long term:

- Define how deception could be part of your detection strategy.
- Deploy in cycles (PLAN - DO - CHECK - ACT).

Choose your destiny

- **General**
  - Get involved in communities and groups focused on Cyber Deception
- **For students**
  - Keep learning, get deeper, take courses
- **For researchers & academics**
  - Do some research, publish papers, build some open-source tools
- **For professionals**
  - Take it into your organization, make small campaigns, try new things

Thank You

If you want to be part of our research

https://forms.gle/7CawihtP8eUU8fe98

CODE: FIRST0625

Find us and get in touch!

Diego Staino	Federico Pacheco
R&D+i Manager	Cybersecurity Services Director
dstaino@base4sec.com	fpacheco@base4sec.com

BASE4
SECURITY