Dogana

ADVANCED SOCIAL ENGINEERING AND VULNERABILITY ASSESMENT FRAMEWORK

Very *fast* overview of the DOGANA project and underlying concepts

25 Jan 2016 - The Hague

E-CRIME Workshop

Enrico Frumento (CEFRIEL), Scientific Coordinator

Twitter: enricoff

CEFRIEL

DIGITAL INNOVATION POLITECNICO DI MILANO


AIT
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY


PROPRS Ltd.


DBI


rath


THALES


CEFRIEL
DIGITAL INNOVATION


inov


cnit


IAI ELTA
ELTA Systems


Dogana
ADVANCED SOCIAL ENGINEERING AND
VULNERABILITY ASSESSMENT FRAMEWORK


Scuola universitaria professionale
della Svizzera italiana
SUPSI


KU LEUVEN


ENGINEERING


Eni


GNS


Hewlett Packard
Enterprise


ΔΗΜΟΚΡΙΤΟΣ
DEMOKRITOS


visionware
your business.our mission


WHERE
WHY
WHEN
?
WHO
HOW
WHAT

What's cybercrime today?

Dogana

From geek-driven to business-driven.

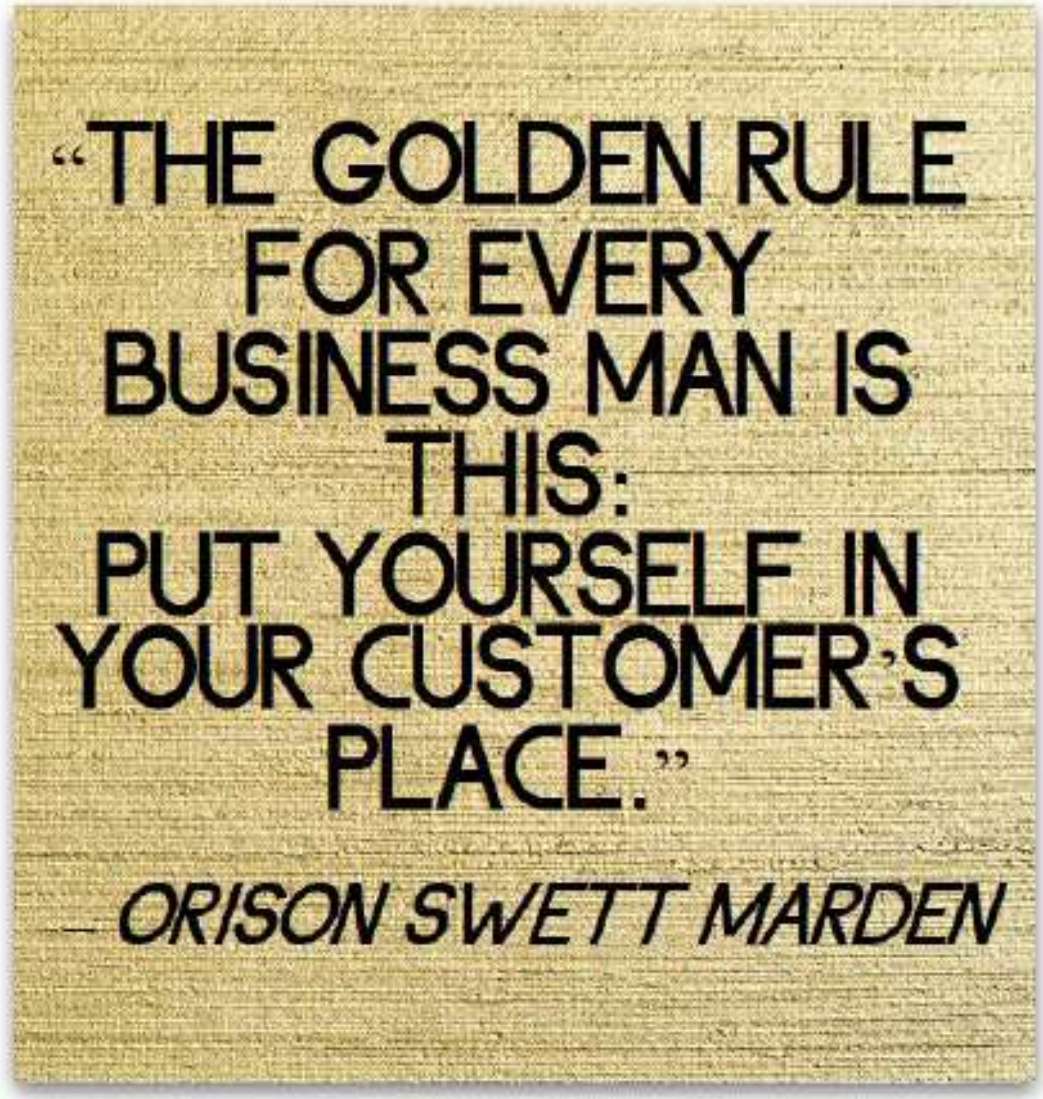
What's cybercrime today?

Dogana

Selling is selling!

What do you need to sell cybercriminals products?

Who's the customer?



What's cybercrime today?

Dogana

What's cybercrime today?

Dogana

YES A TOTALLY DIFFERENT APPROACH, USING THE SAME TECHNIQUES OF MARKETING..

VIRAL,

GUERRILLA,

UNCONVENTIONAL,

... AND OF COURSE SOCIAL

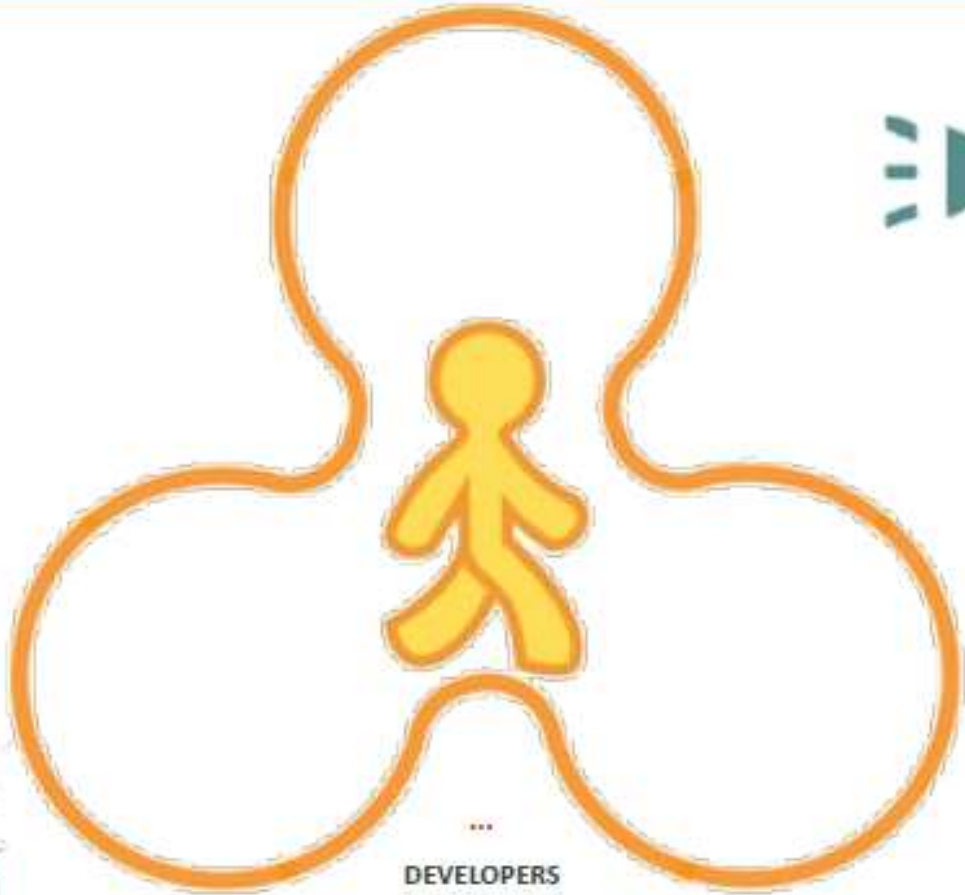
SO WHAT? ANYTHING NEW??

What's cybercrime today?

Dogana

"ADVERTISING"

ADVERTISING



...

DEVELOPERS

SOCIOLOGIST

HCI EXPERTS

PSYCHOLOGIST

SELLERS

MARKETING EXPERTS

SN INFLUENCERS

DOGANA's motivation

- Digital footprint/shadows of companies is often out of control
- Employees awareness level is not know
- Social Media is used daily by many people to share thoughts, images, videos and personal information
- Frictionless/fearless sharing

Exposition over social media

Dogana

At a general level it is possible to identify two main types of exposition over the social media:

Company's exposition

Spread of general and reserved or confidential information regarding projects, products, production sites, etc.

Private user exposition

Spread of personal or working information of a single user (working position, roles, assigned tasks or customers, etc.).

APT

Our experience

Dogana

In the last five years we performed about **20 SDVA** in big enterprises with thousands of employees, involving about **20000 users**

Given an example of a possibile test email

In your opinion, what are the results ?

Overall results

Dogana

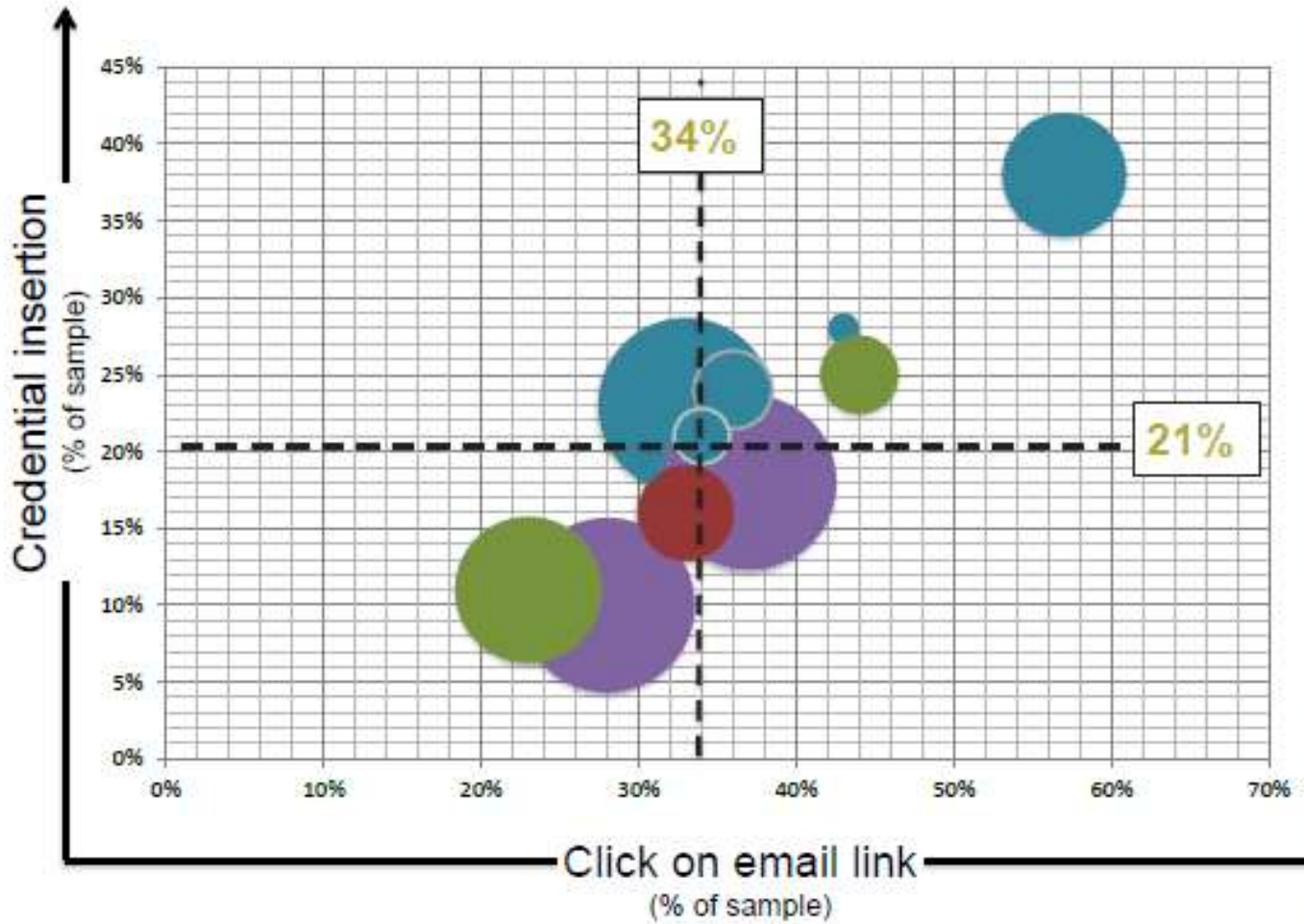
Employees receive the email

34% visit the website

21% also insert the credentials

Benchmarking

Dogana



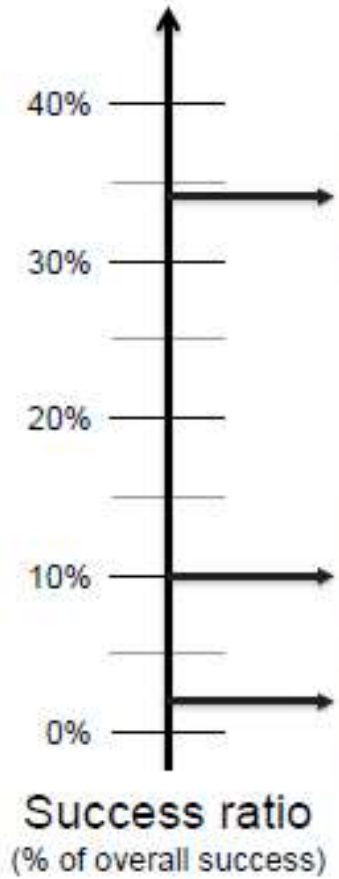
3 emails
to obtain one click

5 emails
to obtain a valid credential

58%
conversion rate
click/insertion

Comparison with other studies

Dogana



34% Average click rate in our research

10% Average click rate in modern phishing

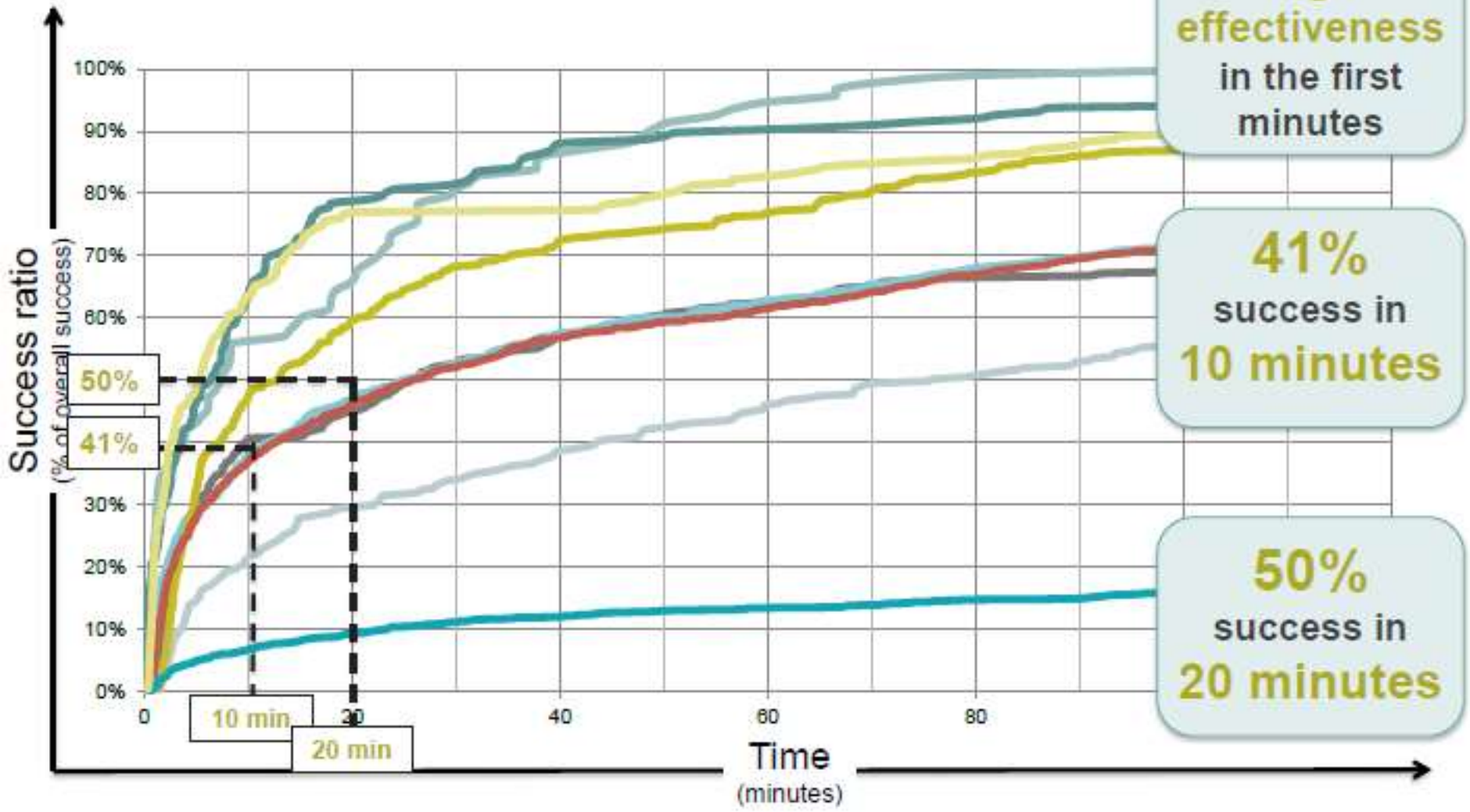
2% Average click rate in Marketing

0,1% Average success in “traditional” phishing

Time analysis - Visits

Dogana

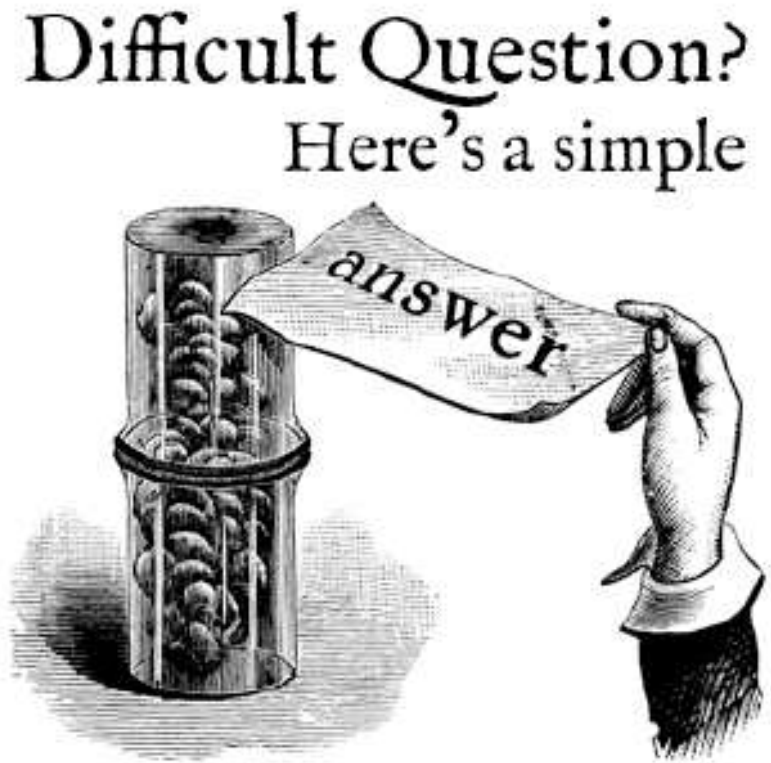
We measure relative effectiveness per campaign



The need: Which countermeasures to use?

Dogana

How can your organisation select the right re-action, given the extreme volatility of these attacks?



The need: Which countermeasures to use?

Dogana

How can the company select the right re-action, given the extreme volatility of these attacks?

Some information cannot be hidden, or can anyway always be rebuilt, or even found elsewhere!

It is very difficult to motivate people or train them against these messages.

To prevent spear phishing, users should not click on Web links or open attachments from unsolicited emails. Organizations should minimize the amount of business-related information, such as job titles, company email, organizational structure, and project names, and personal data being posted on social media Websites. If the information is listed on third-party sites, organizations should contact the site owner and that the data be taken down, according to ICS-CERT.

As for the watering hole attacks, organizations needed to review their policies and requirements for browsing software and ensure common applications are up-to-date with the latest patches.

Policies revision is a slow and complex process, especially in the big enterprises

Updates are sometimes difficult to be delivered due to compatibility reasons (business cannot be interrupted)

The (foreseen) DOGANA answer …

DOGANA plan to deliver a complete toolset to detect and prevent social-engineering cyber-attacks at 3 levels:

- **technological**: develop an integrated toolchain to assist social vulnerability assessments and evolve on the existing tools
- **legal**: supply a legal framework to assist enterprises to perform internally this type of assessments
- **education**: study and experiment new awareness methodologies to improve the education of employees with the aim of a lasting and efficient training.
- **risk management**: measure the risks consistently

The results of the project will be tested with the internal partners enrolled as end-users.

The DOGANA answer …

Dogana

Social Media Scanning

New attack trends

DOGANA Toolset

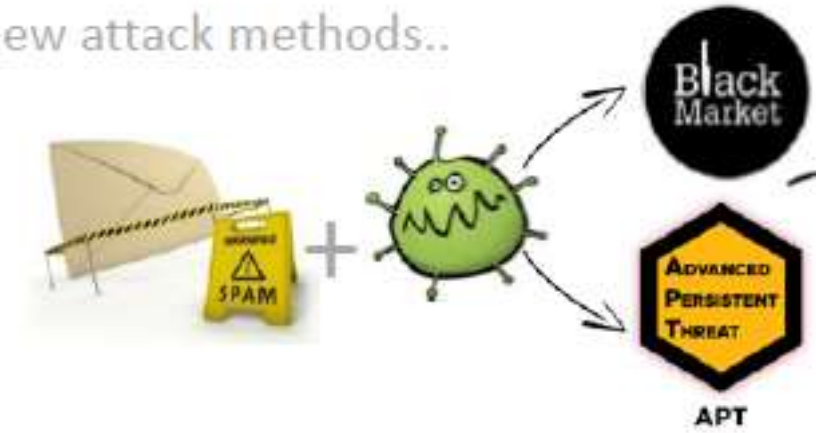
Awareness and new countermeasures

DOGANA delivers a complete toolset to detect and prevent social-engineering cyber-attacks

Pillars of the novel methodology

Dogana

New attack methods..



..require new assessment methods.

Complete Toolset for «social driven» vulnerability assessment

Analysis of web and social medias to evaluate exposure

Google

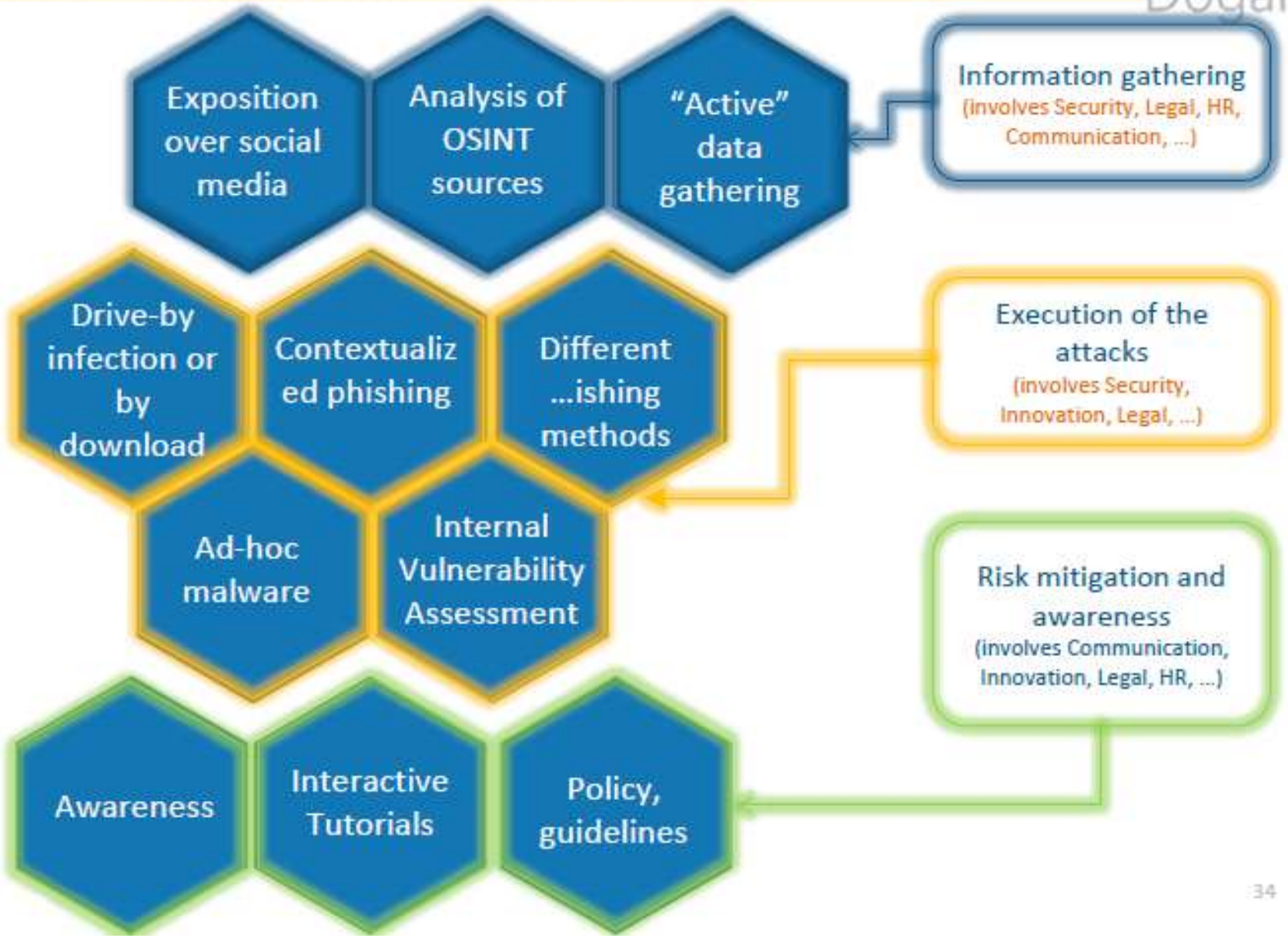
Analysis to select proper profiles

Technological and/or social attack tests, including strongly contextualized

Analysis and assistance to identify and develop solutions

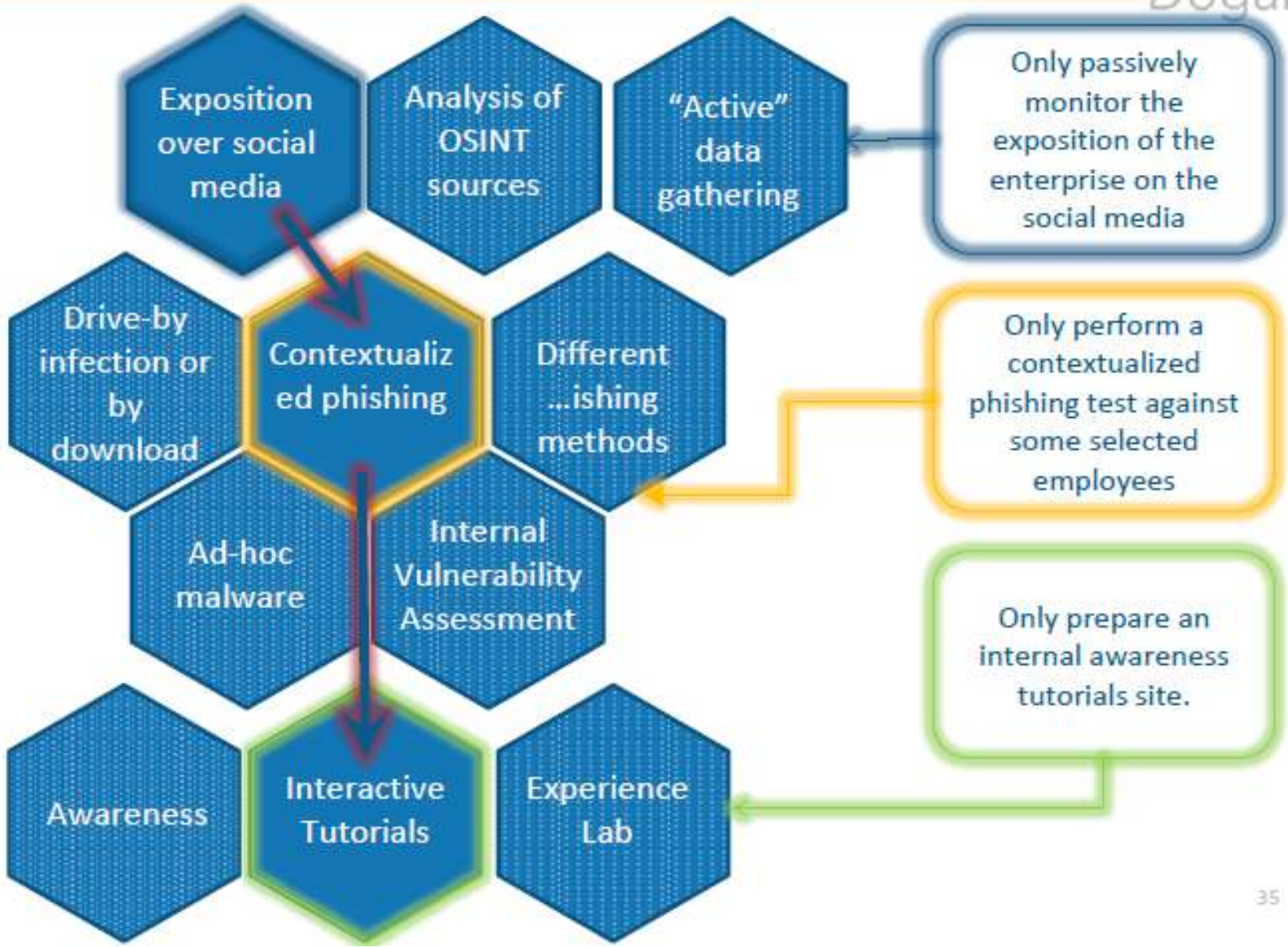
Pillars of the novel methodology

Dogana



Complexity of performing a test-trial a sample

Dogana



CEFRIEL

Via Renato Fucini 2
20133 Milano Italy

tel (+39) 02 23954 1
fax (+39) 02 23954 254

CEFRIEL USA Inc.

Chiquita Center, 15th Floor
250 East Fifth Street
Cincinnati, OH 45202 USA

website: www.cefriel.com

email: info@cefriel.com