aimad.berady@irisa.fr

CARACTÉRISATION TACTIQUE D'UN ATTAQUANT ÉVOLUANT DANS UN RÉSEAU COMPROMIS

SYNTHÈSE DE TRAVAUX DE THÈSE (2018 – 2021)

2021-05-11 / GT SSLR 2021

Aïmad BERADY, V. VIET TRIEM TONG, C. BIDAN, G. GUETTE , M. JAUME

PROBLÉMATIQUE

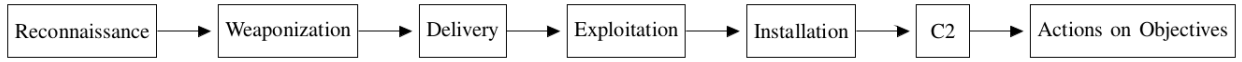
Comment caractériser un attaquant de type APT évoluant dans un réseau compromis ?

QUESTION DE RECHERCHE #1

Quelles sont les différentes phases opérationnelles par lesquelles passe un attaquant au cours d'une campagne ?

MODELING THE OPERATIONAL PHASES OF APT CAMPAIGNS

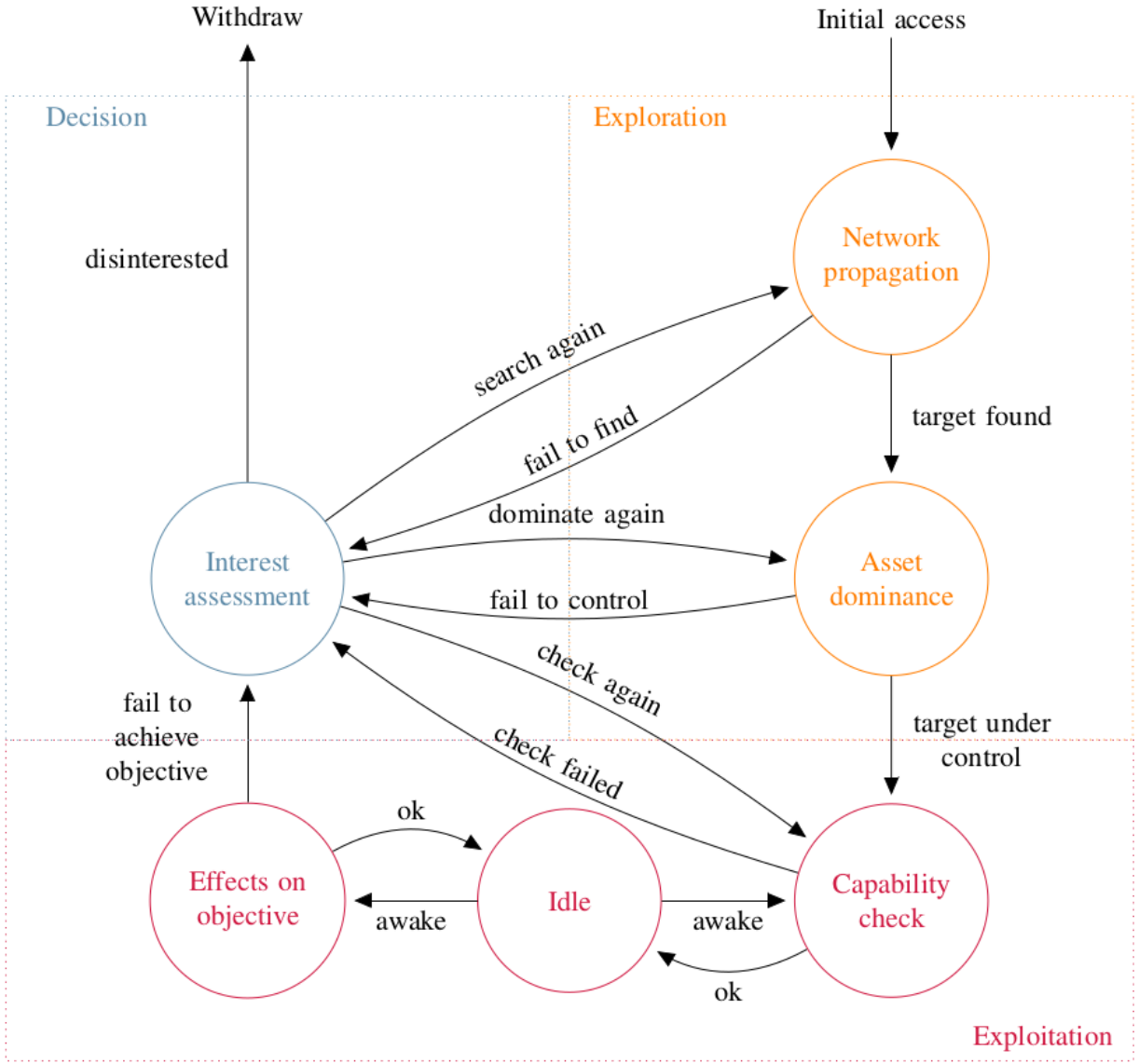
PUBLIÉ DANS IEEE CSCI-ISCW 2019 – HTTPS://HAL.INRIA.FR/HAL-02379869



Lockheed Martin's Cyber Kill Chain[3]

Equifax data breach (2017)[1]

TV5Monde sabotage (2015)[2]



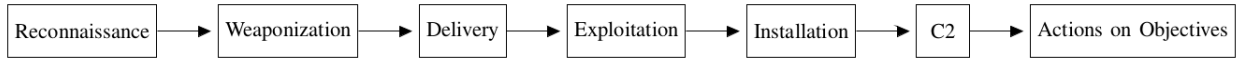
[1] U.S. House of Representatives, "The Equifax Data Breach", pp. 31-39,54, 2018

[2] ANSSI, "Retour technique de l'incident de TV5Monde" [video], 2017

[3] Hutchins, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", 2011

MODELING THE OPERATIONAL PHASES OF APT CAMPAIGNS

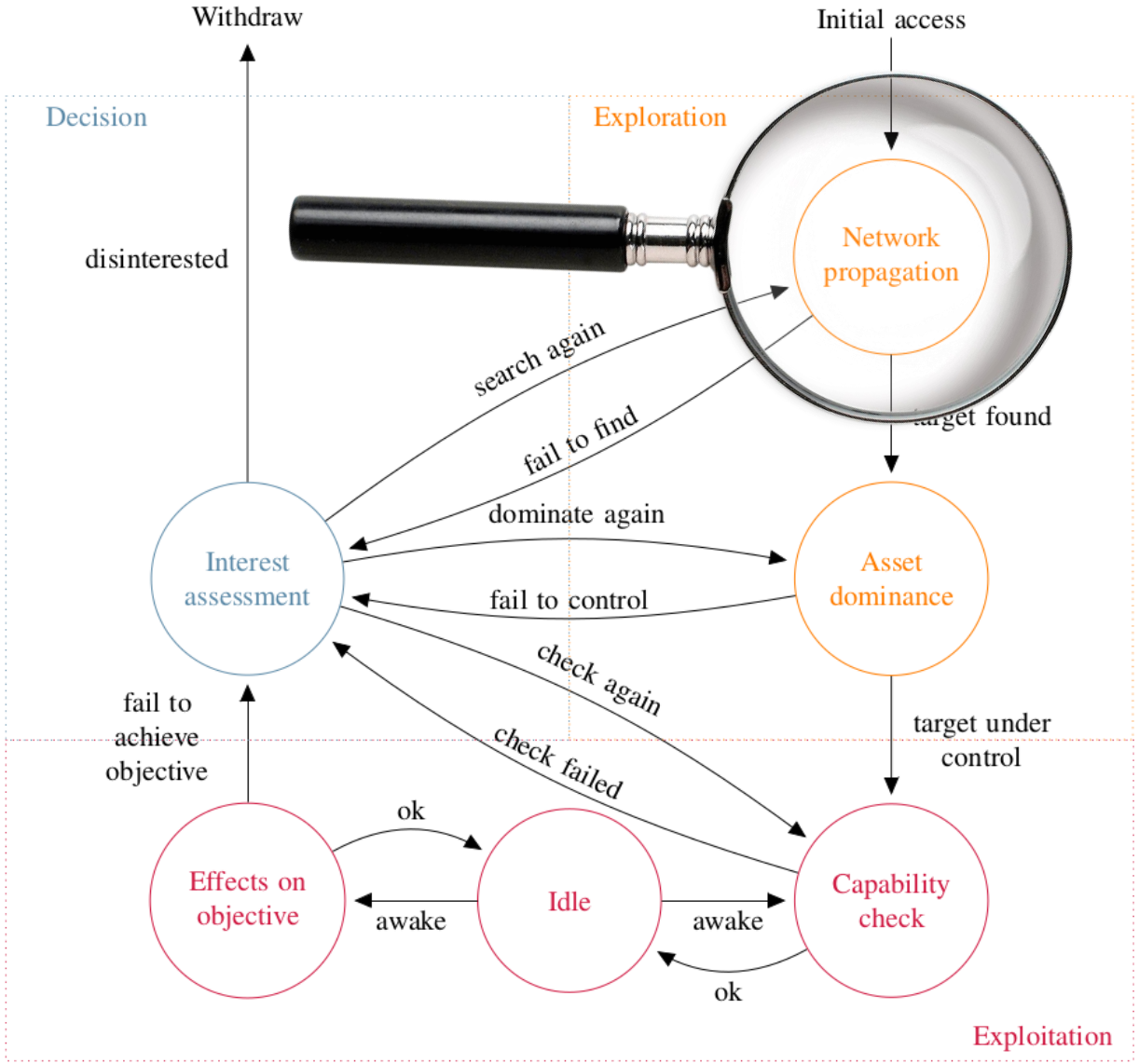
PUBLIÉ DANS IEEE CSCI-ISCW 2019 – HTTPS://HAL.INRIA.FR/HAL-02379869



Lockheed Martin's Cyber Kill Chain[3]

Equifax data breach (2017)[1]

TV5Monde sabotage (2015)[2]



[1] U.S. House of Representatives, "The Equifax Data Breach", pp. 31-39,54, 2018

[2] ANSSI, "Retour technique de l'incident de TV5Monde" [video], 2017

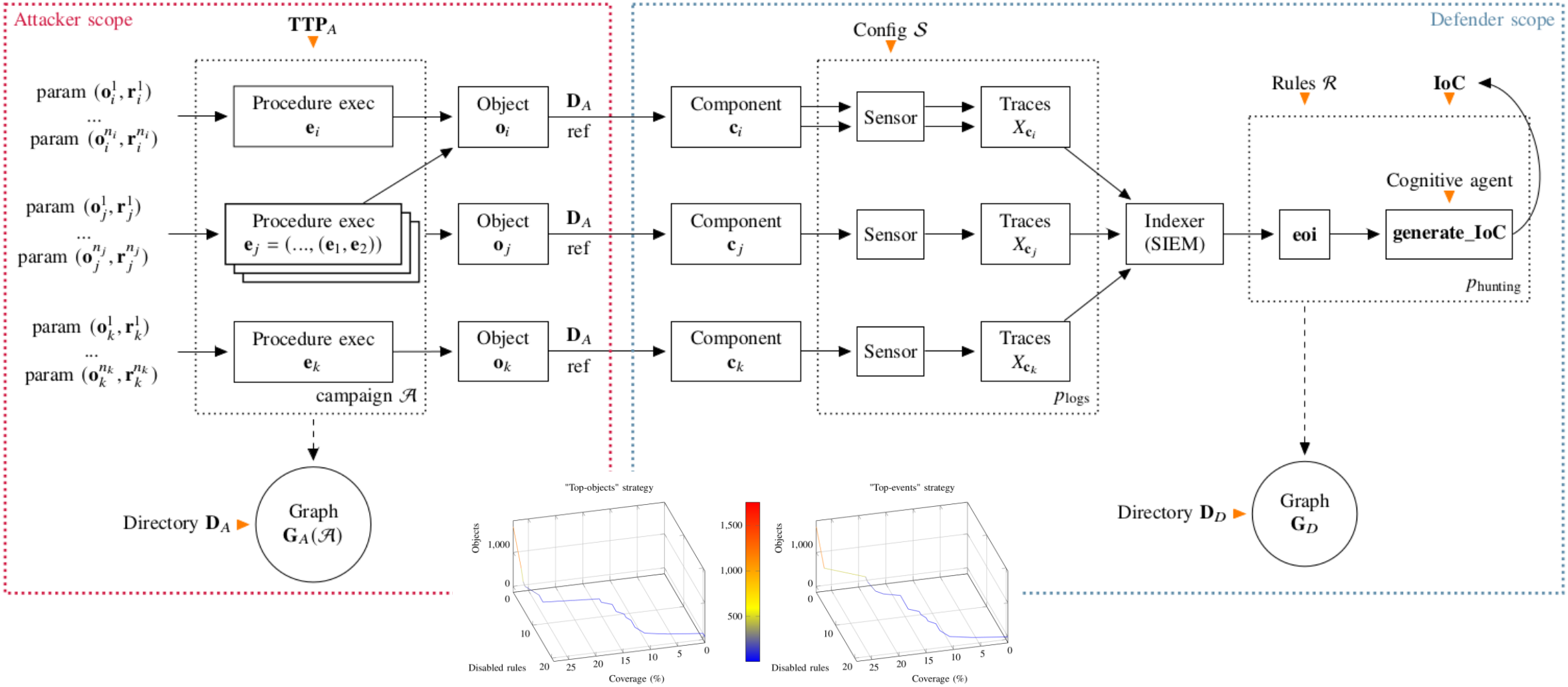
[3] Hutchins, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", 2011

QUESTION DE RECHERCHE #2

Que partagent l'attaquant et le défenseur dans leurs perceptions respectives d'une campagne ?

FROM TTP TO IOC: ADVANCED PERSISTENT GRAPHS FOR THREAT HUNTING

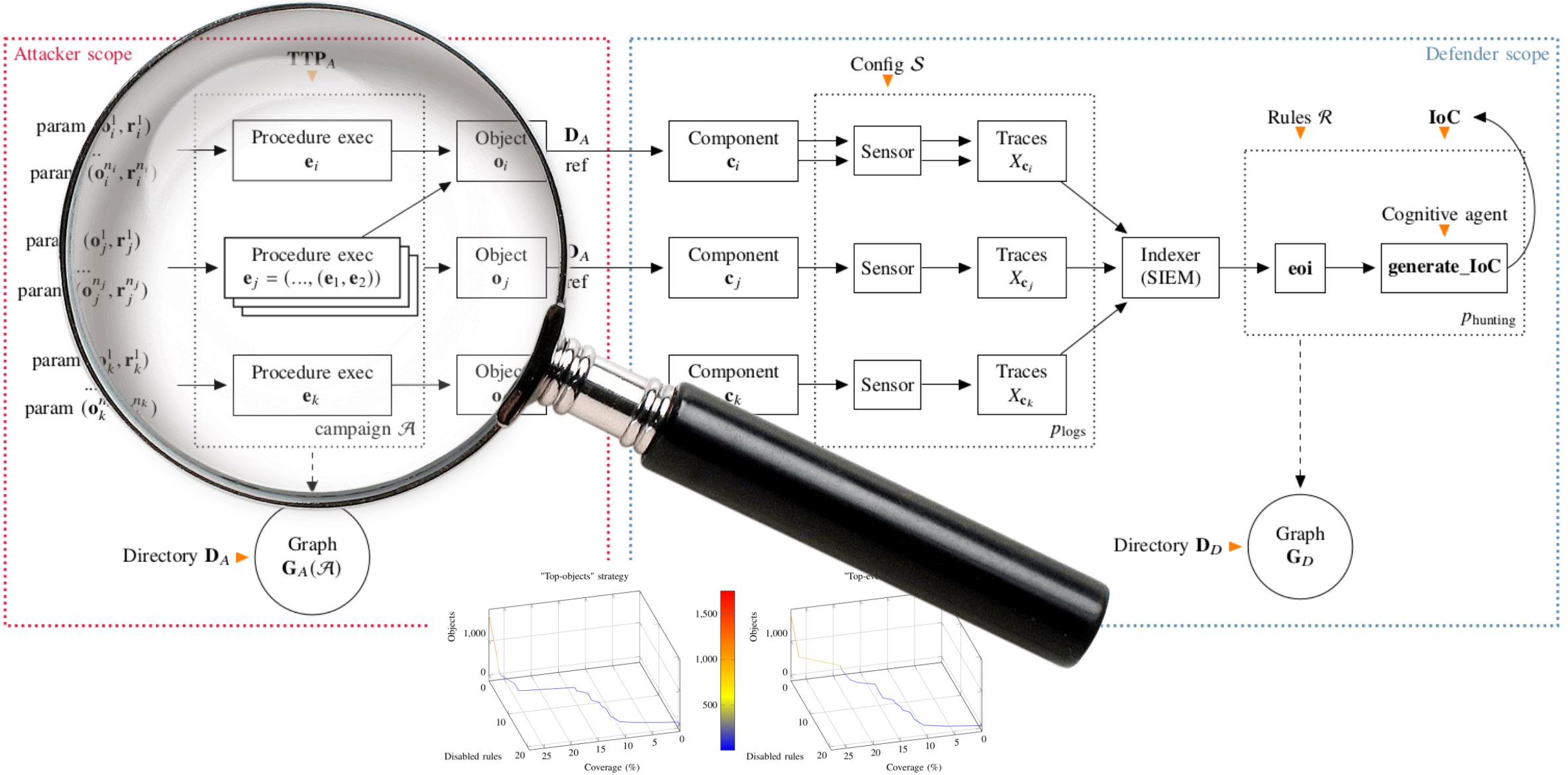
PUBLIÉ DANS IEEE TNSM 2021 – HTTPS://HAL.INRIA.FR/HAL-03131262



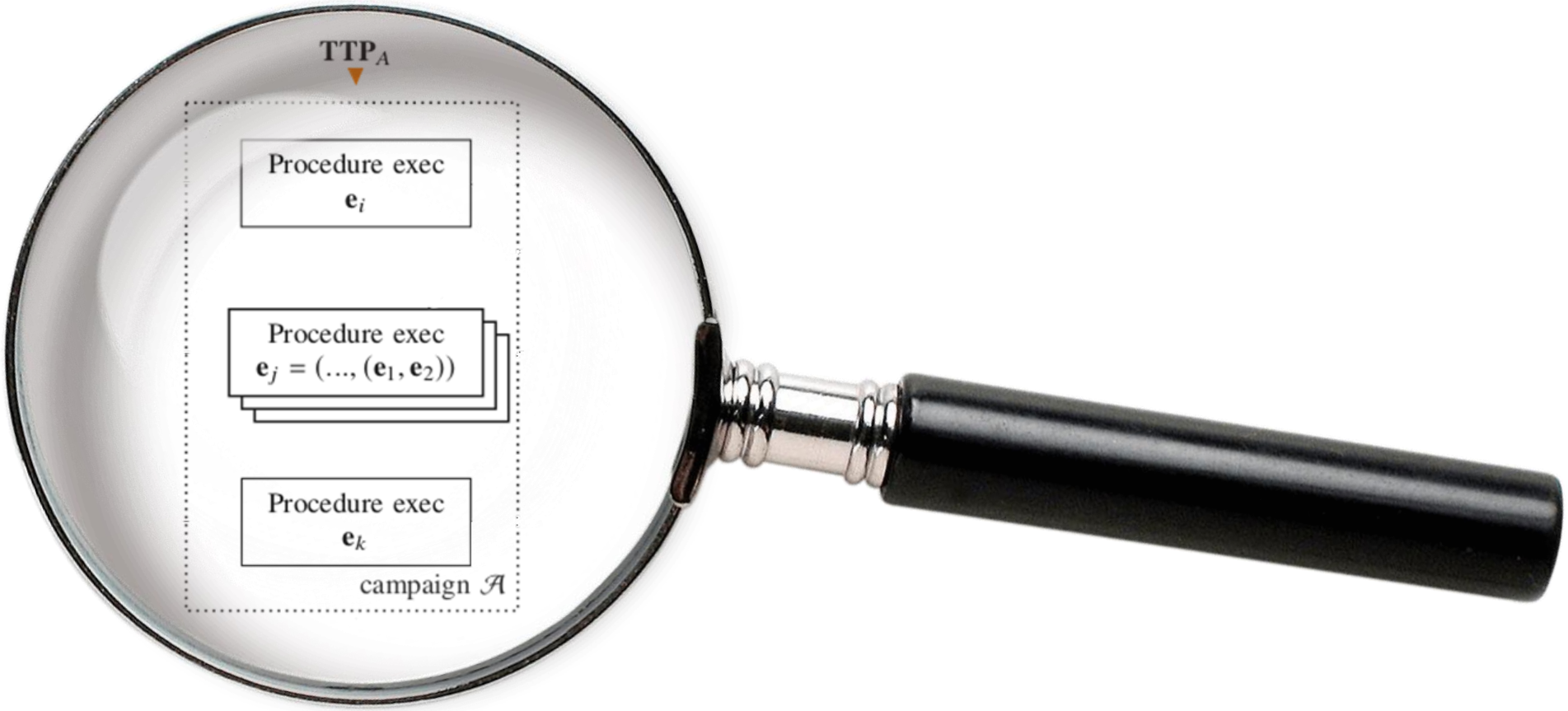
MORDOR PROJECT : https://github.com/OTRF/mordor/tree/master/datasets/large/apt29

FROM TTP TO IOC: ADVANCED PERSISTENT GRAPHS FOR THREAT HUNTING

PUBLIÉ DANS IEEE TNSM 2021 – [HTTPS://HAL.INRIA.FR/HAL-03131262](https://hal.inria.fr/hal-03131262)



QUESTION DE RECHERCHE #3



Comment se comporte un attaquant au cours de sa progression dans un réseau compromis ?

YES WE H/CK PWNJUTSU IRSN

PWNJUTSU : EXPÉRIMENTATION SUR LE COMPORTEMENT D'UN ATTAQUANT