



HAL
open science

Preparing & Responding to Cyber Incident Crisis in Healthcare: Design and Development of technical training capabilities implementing theoretical & practical methods

Nasir-Baba Ahmed, Gilles Dusserre

► To cite this version:

Nasir-Baba Ahmed, Gilles Dusserre. Preparing & Responding to Cyber Incident Crisis in Healthcare: Design and Development of technical training capabilities implementing theoretical & practical methods. Colloque IMT 2023 : “ Sécurité et Résilience ”, Apr 2023, Palaiseau, France. 2023, <10.5281/zenodo.7937270>. <hal-04097891>

HAL Id: hal-04097891

<https://imt-mines-ales.hal.science/hal-04097891v1>

Submitted on 15 May 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

Preparing & Responding to Cyber Incident Crisis in Healthcare:

Design and Development of technical training capabilities implementing theoretical & practical methods

Authors

Nasir Baba AHMED
Gilles DUSSERRE

Partners



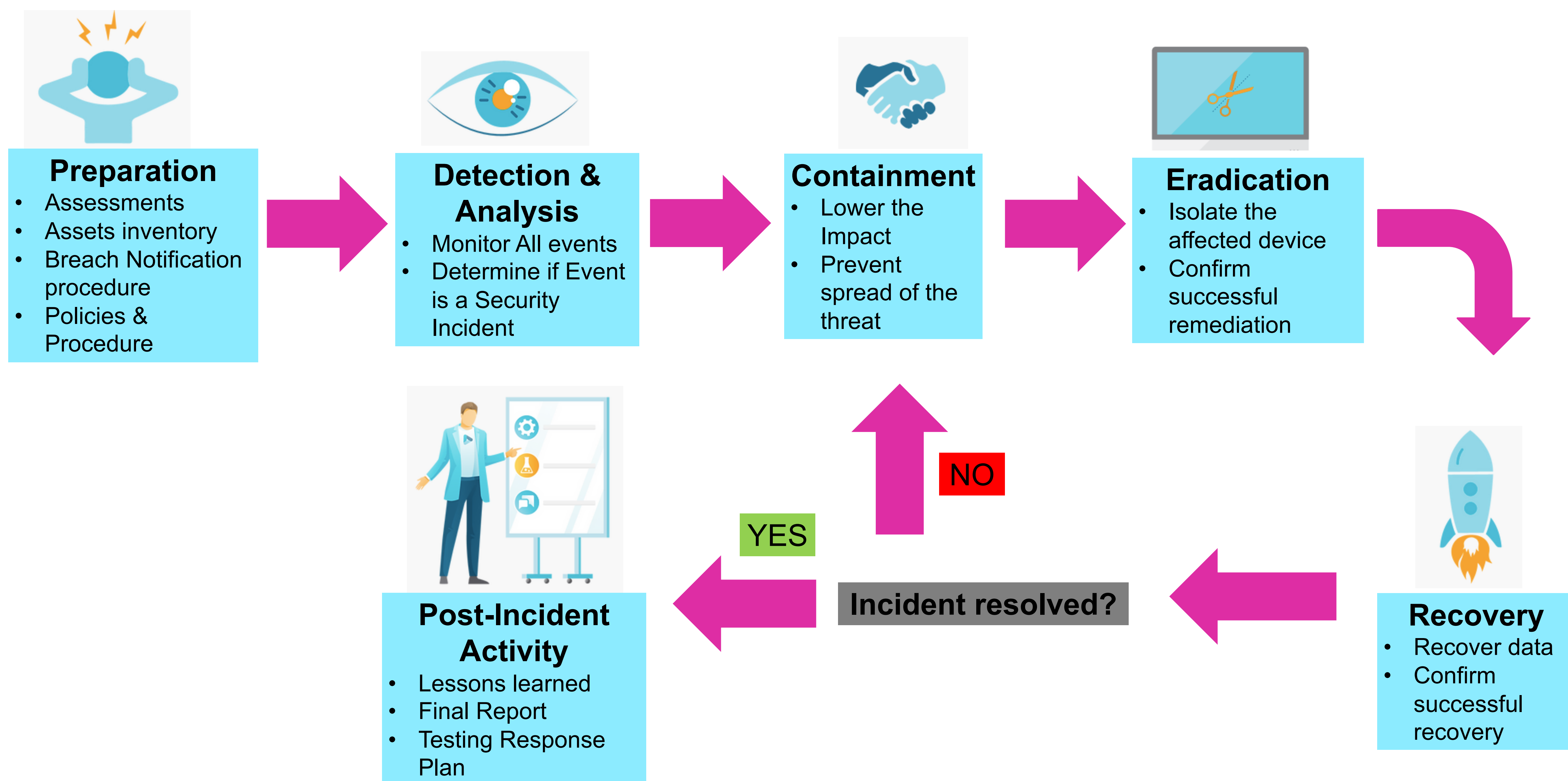
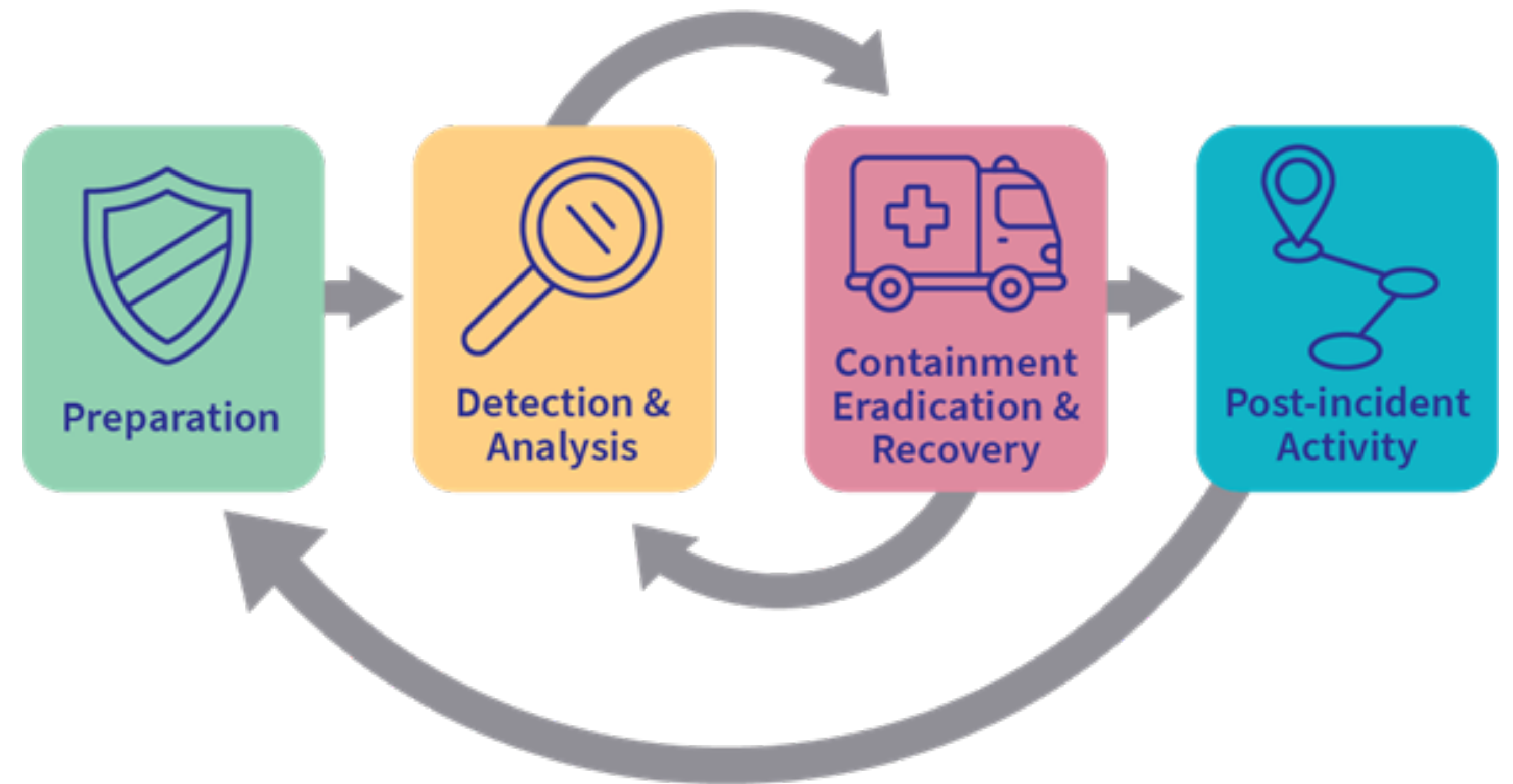
IMT Mines Ales



Telecom SudParis

CONTEXT & GAP:

- ▶ **Rise in Cyber Incidents:** Cyberattacks targeting hospitals in France particularly have been rising with 380 cases reported last year, 66% of healthcare organizations surveyed were attacked in 2021, up from 34% in 2020. This is a 94% increase over the course of a year (*Sophos, 2022*)
- ▶ **Shortage in Cybersecurity Experts:** The global cybersecurity workforce show a need for more than 3.4 million cyber security professionals, an increase of over 26% from 2021's numbers (*ISC2, 2021*)



RESEARCH OBJECTIVES:

- ▶ **Evaluation** of the **Cyber Incident Response** in healthcare cyber infrastructure, and its organizational operations.
- ▶ **Deliver and improve the Cyber Incident Response methods** (standardised) to assist healthcare and other organisational responding effectively to any cyber crisis situation.

RESEARCH OUTCOMES:

- ▶ Prepare Quality, and world class level Incident response materials
- ▶ **Training** for the next generation of cyber experts in incident response
- ▶ **Structured Approach** to usage of Theoretical use cases & Practical - (including: Setup & usage of technical tools/techniques)
- ▶ Recommendations for **Annual review and improvement of Process**
- ▶ Recommendations for **Extra Guidelines/materials for extra research**
- ▶ **Delivery** in a highly interactive method to encourage engagements

