USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

CTO PEER MENTORING PROGRAM

Topic 1 Mentor Session

Introduction

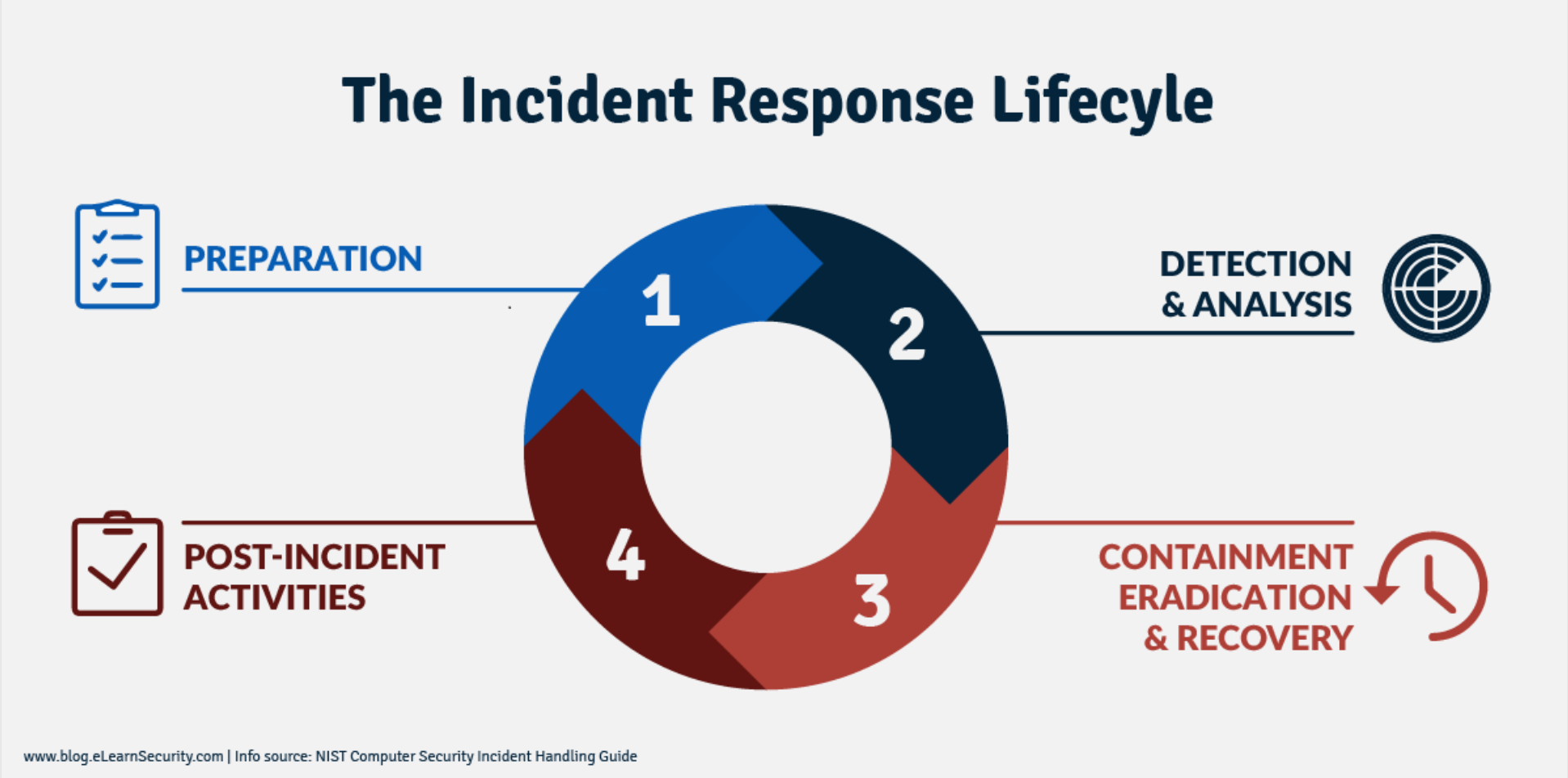
This publication was produced at the request of the the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

DEVELOPMENT OF AN ORGANIZATIONAL INCIDENT RESPONSE PLAN FOR RESPONDING TO THREATS

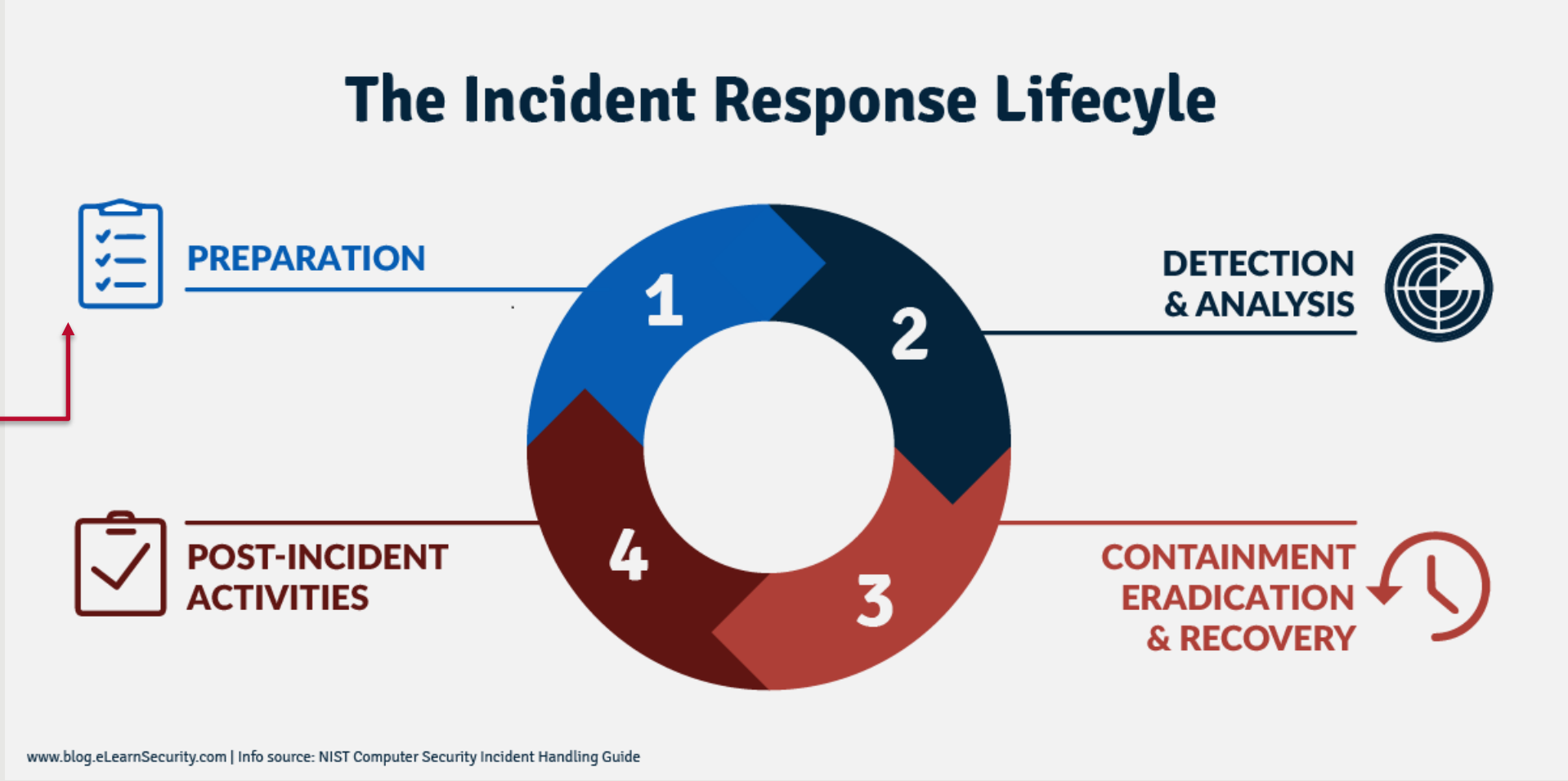
USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Presentation Disclaimer

INCIDENT RESPONSE PLANNING



IS INCIDENT RESPONSE STATIC, OR A "ONCE-OFF" EXERCISE?



Topic 1

COMPROMISE EXAMPLES LEADING TO INCIDENT RESPONSE FAILURES

NotPetya – 2017

Global Engineering & Industrial Manufacturing Organization

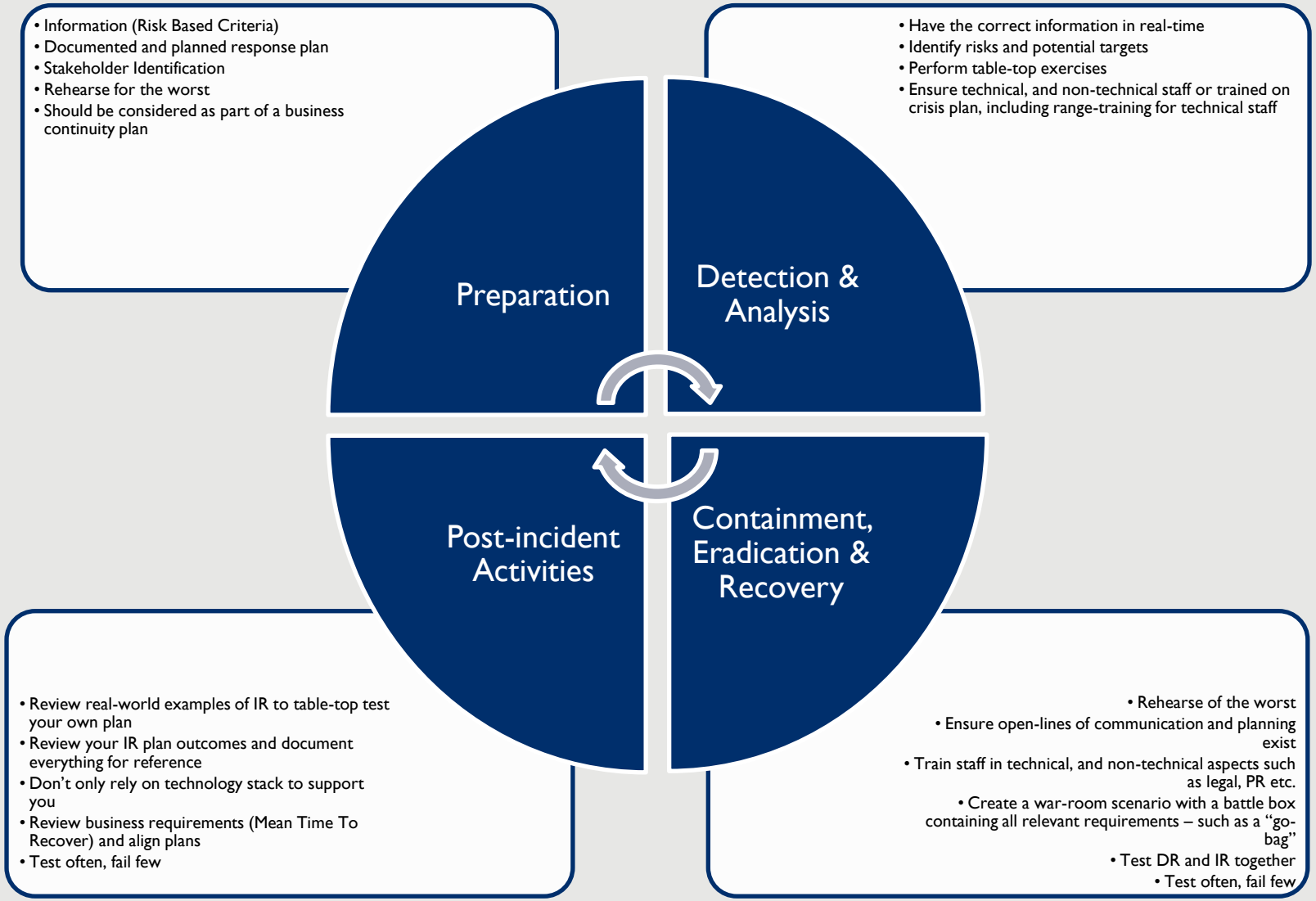
- $30.0+ Million Business spanning 6 Continents
- No Incident Response Planning or Ability to Prevent Attack holistically
- Globally downed for 1.5 Months (MTTR)
- Ongoing estimated loss of $1 000 000.00 per continent, in productivity and work hours

Targeted Attack – 2018 to 2019

African Construction & Supply Manufacturing Giant

- $665.0+ Million Business spanning 10+ Countries
- Targeted Attack highlighting failure in Detection & Analysis, taking place over 2 years
- Documented Incident Response & Business Continuity Plan only, with no practical application or testing
- Estimated Loss of $22 500 000.00 across Ransom, Intellectual Property Theft/Other Data Leaks, Reputational Damage, Professional Liability, Employee Personal Liability

EXPERIENCE HAS LED US TO BELIEVE…



USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

QUESTIONS AND ANSWERS

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

SCENARIO 1:

How would you implement incident response for an organization which has just discovered that they are compromised? What are the key items which you would address and prioritize?

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

SCENARIO 2:

Where would you start designing an incident response plan for an organization which has no plan in place? What are the first priorities which you would address, and what methodology would you utilize?

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

QUESTIONS AND ANSWERS