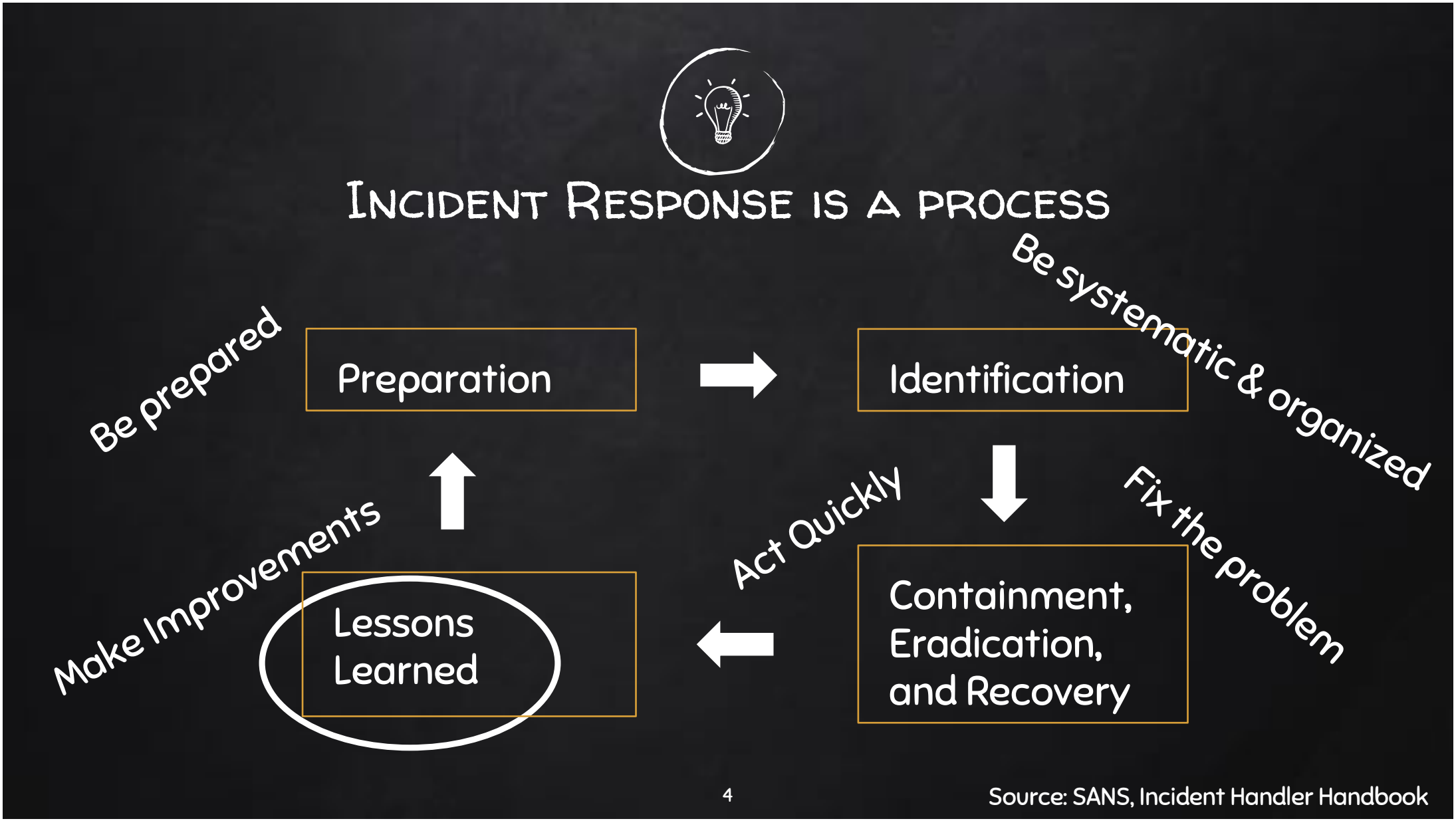

Learning From Incident
5th cdef meetup
Ferry Afit K
CYBERSOC
TELKOM

Skyfall “He hacked us” scene


WELCOME TO INCIDENT RESPONSE
imgflip.com


Incident Response is a process
Be prepared
Preparation
Identification
Be systematic & organized
Act Quickly
Fix the problem
Containment, Eradication, and Recovery
Lessons Learned
Make Improvements
Source: SANS, Incident Handler Handbook

- ✗ Incident of all sizes happen every day
- ✗ Preparation could mean the difference between success and failure


ATTACK
ATTACK EVERYWHERE

Content only available on meetup


experience is
the best
teacher

- ✗ Learn from the experience of others
  - Threat trends
    - Telegram Channel @secnewsfeeds
  - Presumptions of compromise*
- ✗ Every security incident is an opportunity to improve
  - People: awareness
  - Process: procedure
  - Technology: more use case, alert system

Learn from other people's mistakes. Life is too short to make them all yourself.

— Sam Levenson —

AZ QUOTES

SUMMARY

- ✗ Being prepared for incident response (IR) is likely to be one of the more cost-effective security measures any organization can take.
- ✗ Every security incident is an opportunity to improve

IR needs people, because successful IR requires thinking

–

Anton Chuvakin

Reference

- Computer Security Incident Handling Guide, NIST SP 800-61r2
- The Incident Handlers Handbook, SANS
- How to Plan and Execute Modern Security Incident Response, Gartner

THANKS!