NIS/ NIS 2

Global specifications; Industry Specific Implemention

Moussa OUEDRAOGO

Head of Cybersecurity Services

FUJITSU

Agenda

FUJITSU

NIS/ NIS 2:

Global specifications, industry specific implemention

- BACKGROUND – VITAL & ESSENTIAL SERVICES
- Principle 1: Risk management and Supply Chain
- Principle 2: Event detection and attacks mitigation
- Principle 3: Ensuring Continuity

BACKGROUND VITAL & ESSENTIAL SERVICES

Critical Services, Insecure Systems

FUJITSU

Letting the demons in...

TRANSPORT

ENERGY & WATER

HEALTHCARE

Critical Services, Insecure Systems

FUJITSU

Letting the demons in...

TRANSPORT

ENERGY & WATER

ICT NETWORK

HEALTHCARE

Bottomline: if it is not secure, it is unlikely to be safe

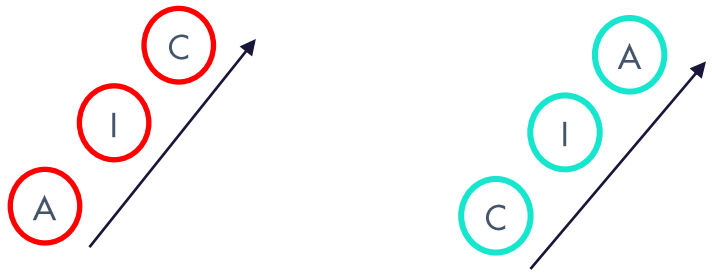
Digital Vs Control Systems

A tale of two worlds

FUJITSU

Security Objectives

ICT	ICS



Malwares Protection

ICT	ICS
Common	Difficult

Technology

ICT	ICS
Standardised & "Controlled Security	Proprietary & Insecure

Impact Scope

ICT	ICS
Financial & Non-tangible	Health & Safety

A forest of Standard & Guidelines

FUJITSU

What to consider as reference?

...

NIS(2) Regulation

What & Who

OBJECTIVES

- Protect Against Cyber Attacks & minimise effects
- Managing Security Risk
- Minimise the Effects of Cyber Security Incidents
- Supply chain risk management
- Management accountability

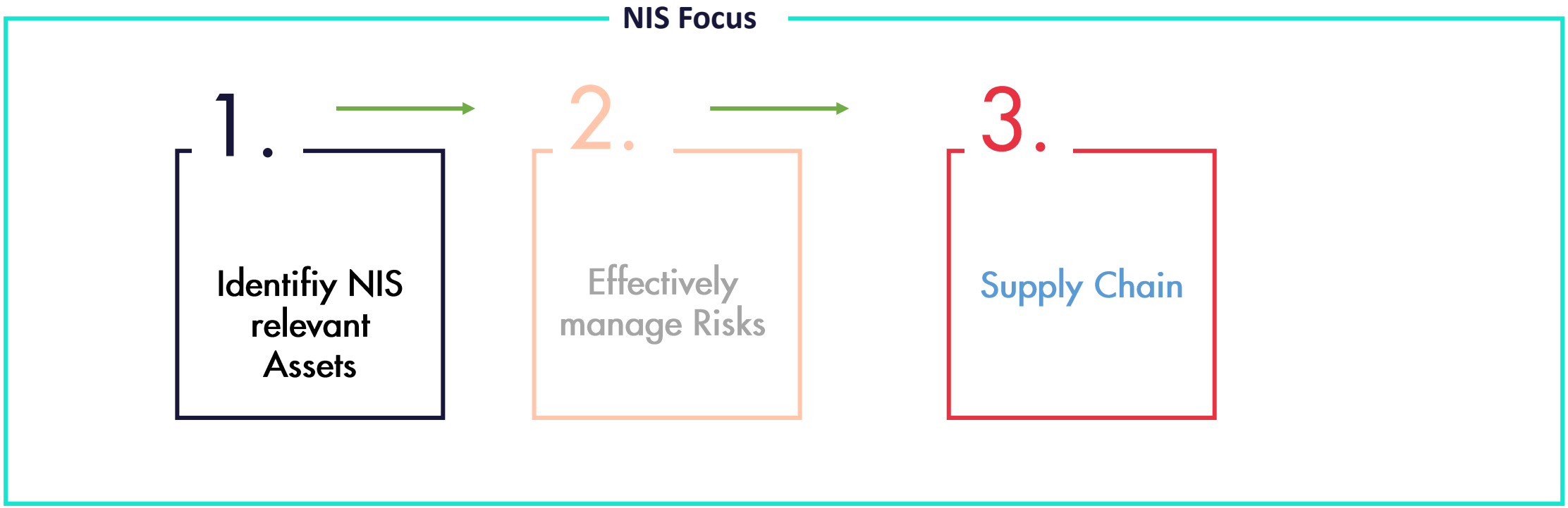
WHO



Managing Security Risk & Supply chain

Principle # 1

Managing Cybersecurity Risks

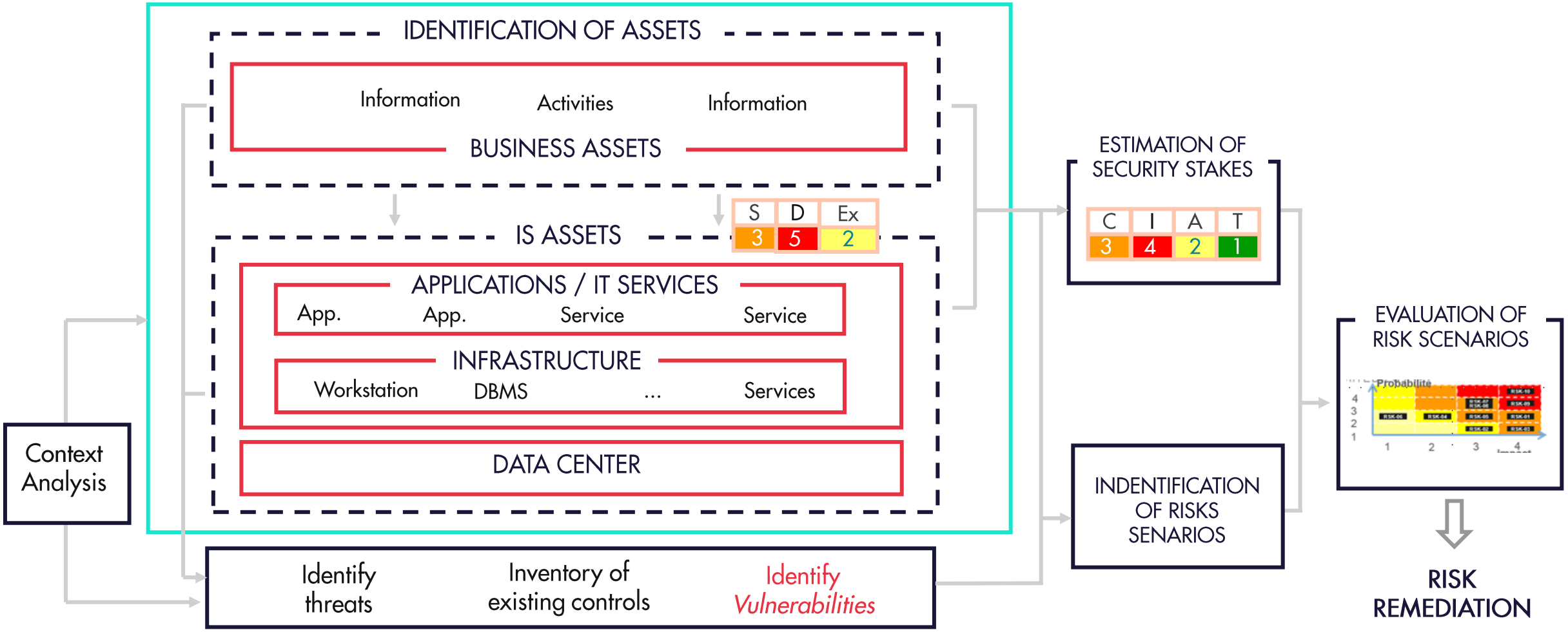


Principle # 1

[E|V] Asset Management

Risk management

Do you know your risk ?



Principle #1

Managing Cybersecurity risks

FUJITSU

General risk management

ISO 27005 EBIOS COBIT

NIST 800-37 SANS MONARC ...

Recommanded/Mandated

TISRIM

Domain Specific

ISO 14971 (Healthcare)

IEC 62443 Serie (ICS & Energy)

EUROCAE ED-20x (Air transport)

CENELEC prTS 50701 (Railways Services)

Principle # 1

Supply Chain, the new weakest Link

- Know your supplier cybersecurity maturity
- Set thresolds for acceptance, before you integrate
- Share your Cybersecurity standards and ensure they are integrated in development of products and services
- Efficient vulnerability management
- Check latest NIST SP 800-161r1

2

FUJITSU

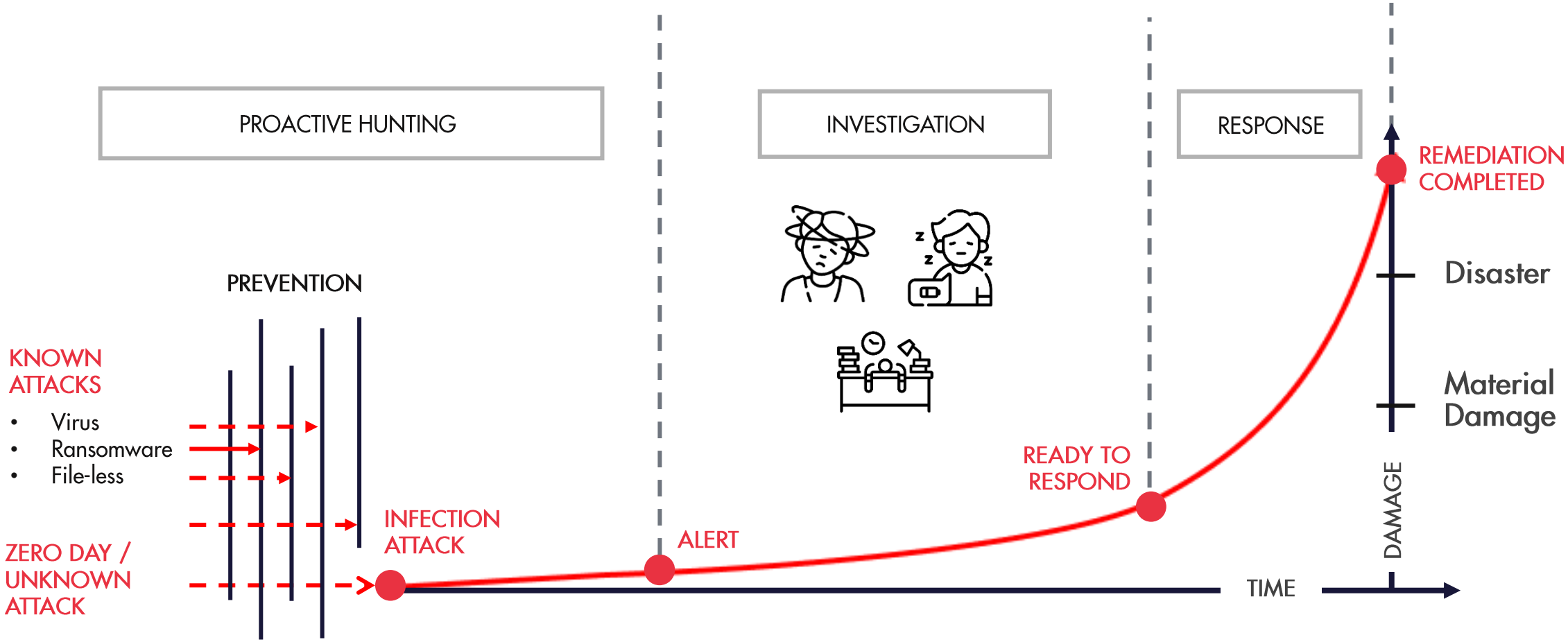
Attacks

Detecting events & minimizing attacks effects

Principle # 2

FUJITSU

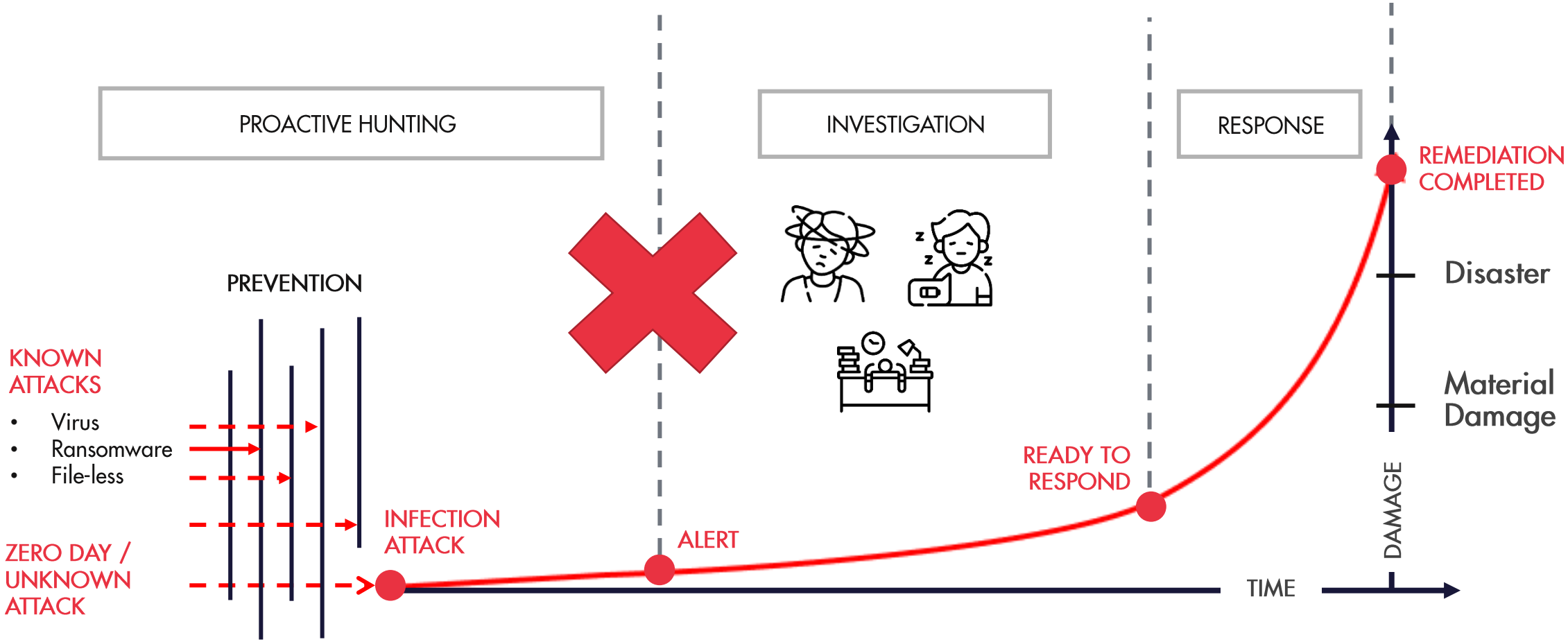
Detection means: Going beyond current practices



Principle # 2

FUJITSU

Detection means: Going beyond current practices



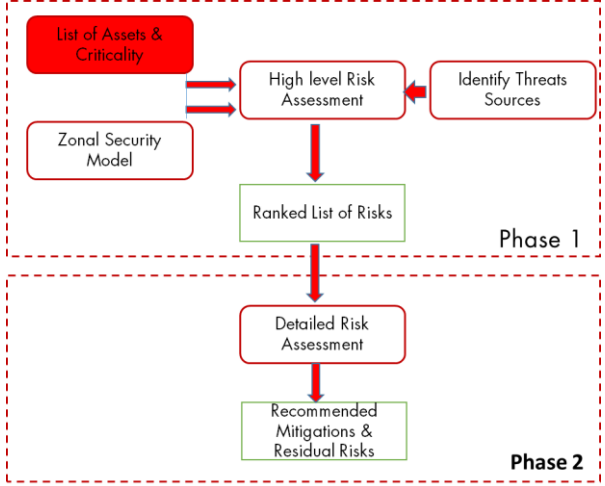
Principle # 2

Minimising the effect of Attacks

- Importance of that Asset

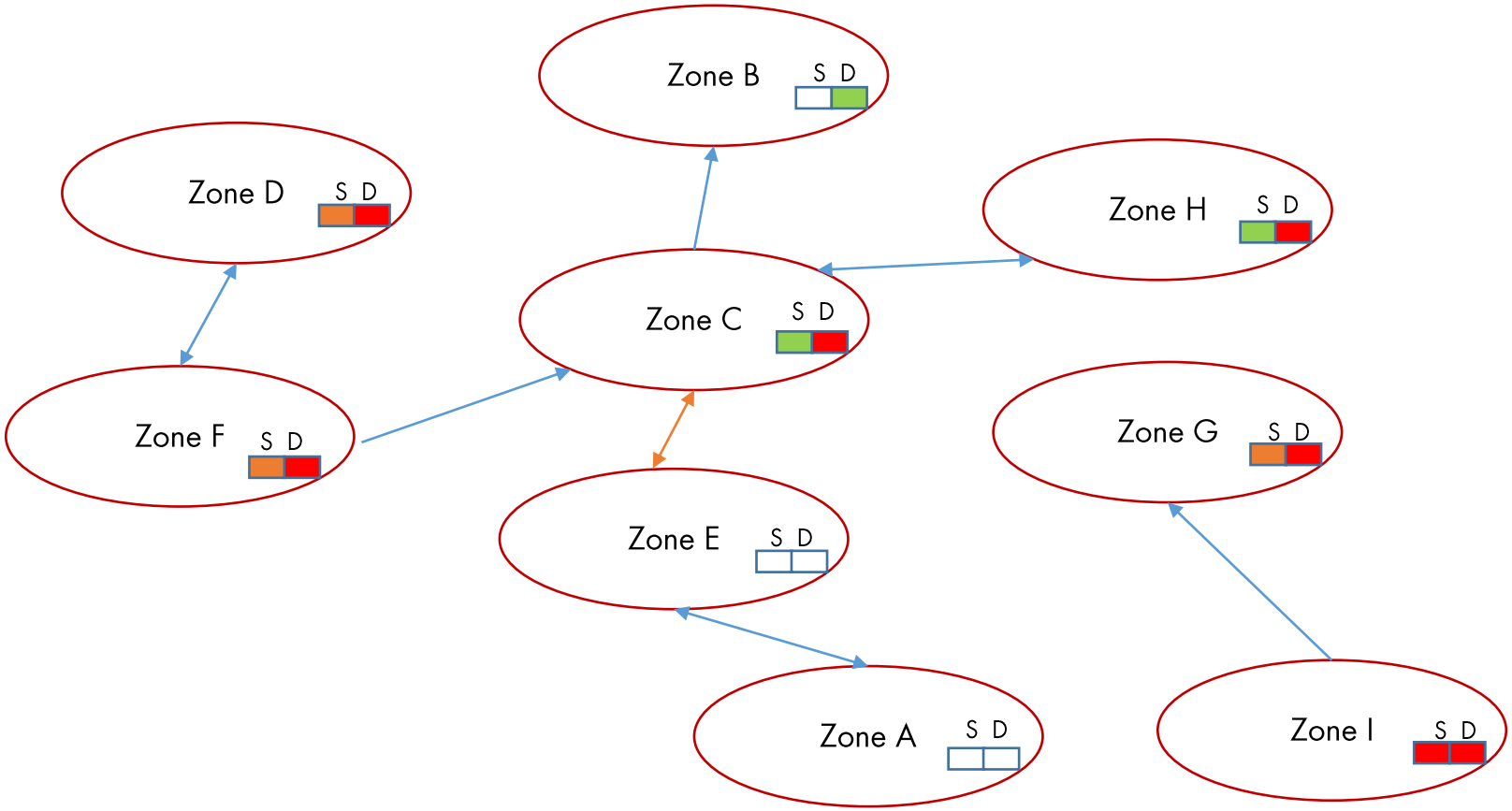
- Security level for each asset

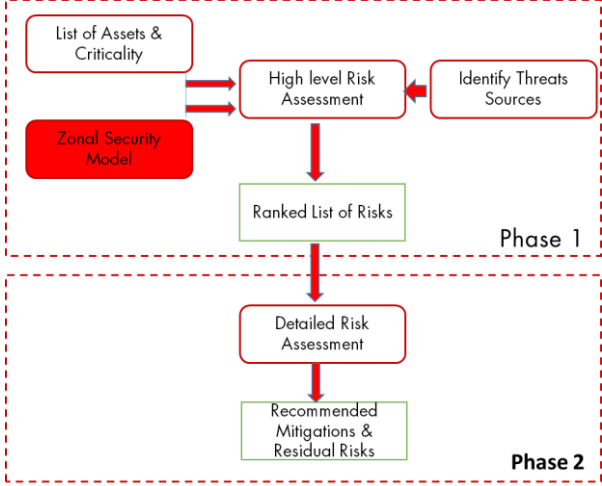
- Threats sources



Minimising the effect of Attacks

Zonal Security





S: Heath&Safety D:Disruption

3

GEARING UP

For recovery

Principle #3

Continuity and Crisis Management

FUJITSU

"How prepared are you to face up a major attack ?"

- Resilience and Preparedness
  - Resilience based Cybersecurity
  - Business Continuity Planning and Strategy
  - Disaster Recovery Planning
- Management cyber crisis
  - Building pragmatic scenarios
  - Test your Preparedness
  - Coordination of your response


Thank you
FUJITSU