34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

Ivan Taylor and Keith Willett

Modelling Cybersecurity Operations to Improve Resilience

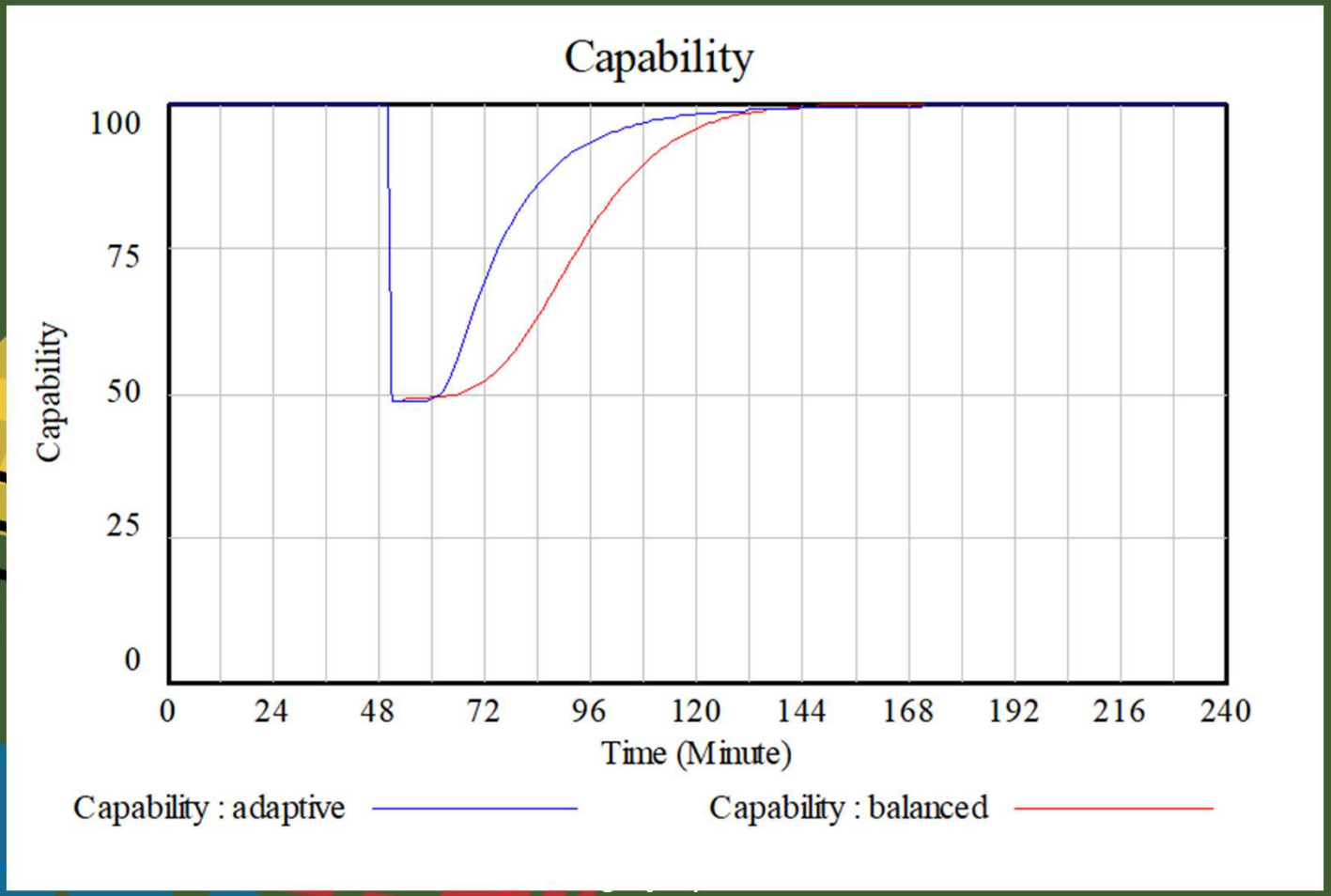
Outline

- Introduction
- System Dynamics Model
- Case Study Results and Implications
- Key Takeaways.

Introduction

- Resilience is the ability to avoid, withstand, or recover from adversity.
- Network Security Operations Center (NSOC)
- Resilience will be explored through a case study
- Restoring a system's capability after a cyber-attack
- Balanced and Adaptive allocation of human resources

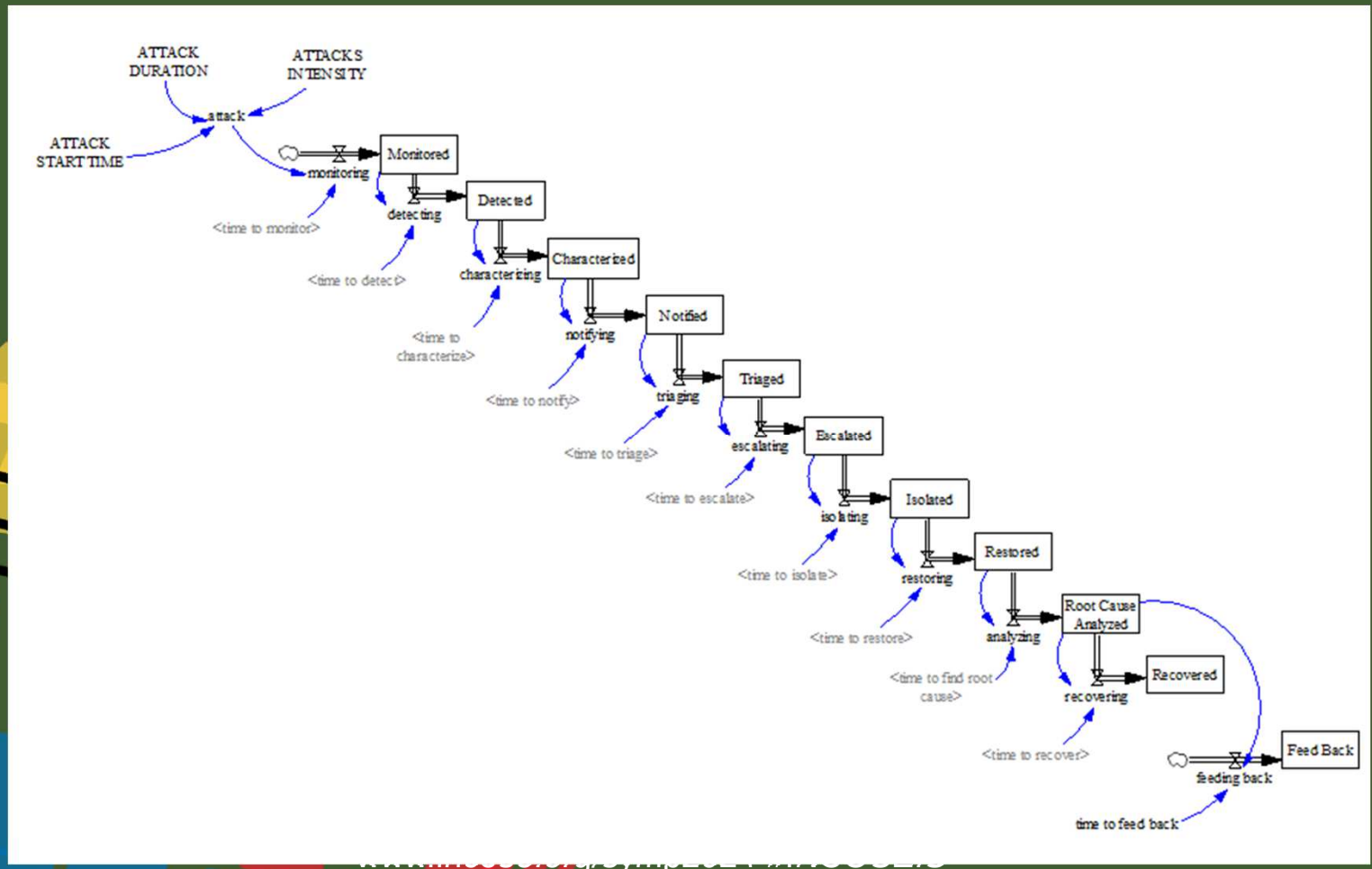
Capability with Balanced and Adaptive Resource Allocations



Cybersecurity Operations Phases

Phase	Description
Monitor	Ongoing observation with intent to raise awareness
Detect	Indicator of anomaly where an anomaly is something unexpected
Characterize	Known-known, known-unknown, unknown-unknown, unknown-known
Notify	Tiered support
Triage	Determine priorities
Escalate	Send to subject matter expert(s)
Isolate	Contain adversity or effects of adversity
Restore	Restore effective operations even if at diminished capacity
Root Cause Analysis	Identify the root cause of the problem
Recover	Recover operations to *desired* performance level
Feedback	Minimize anomaly/adversity recurrence and effects of recurrence

Cascade System Dynamics Model



System Dynamics Model

System Dynamics models are based on highly interconnected first-order differential equations solved using numerical integration.

$Q_j(t)$ represents the number of tasks in the process j at time t,

$I_j(t)$ represents the number of incoming tasks to process j at time t and

$O_j(t)$ Represents the completion or outflow of tasks from the process j at time t.

T_j is based on the resources available at the process j.

$$Q_j(t) = \int_0^t \left(I_j(t) - O_j(t)\right) dx + Q_j(0)$$

$$I_j(t) = Q_{j-1}(t) / T_{j-1}$$

$$O_j(t) = Q_j(t) / T_j$$

Resource Allocation Strategies

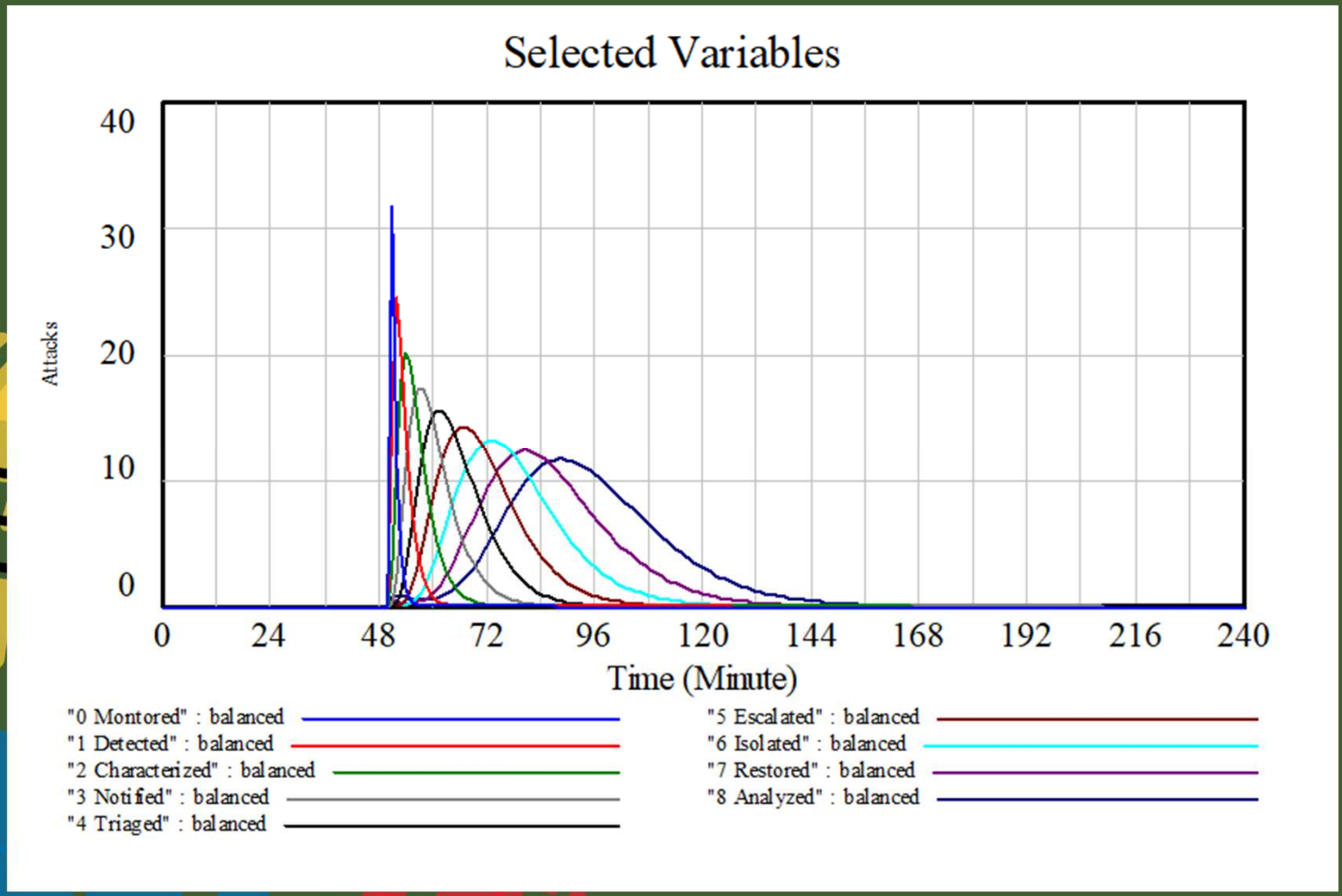
Balanced

- Each process is allocated the same level of human resources as in a siloed organization.

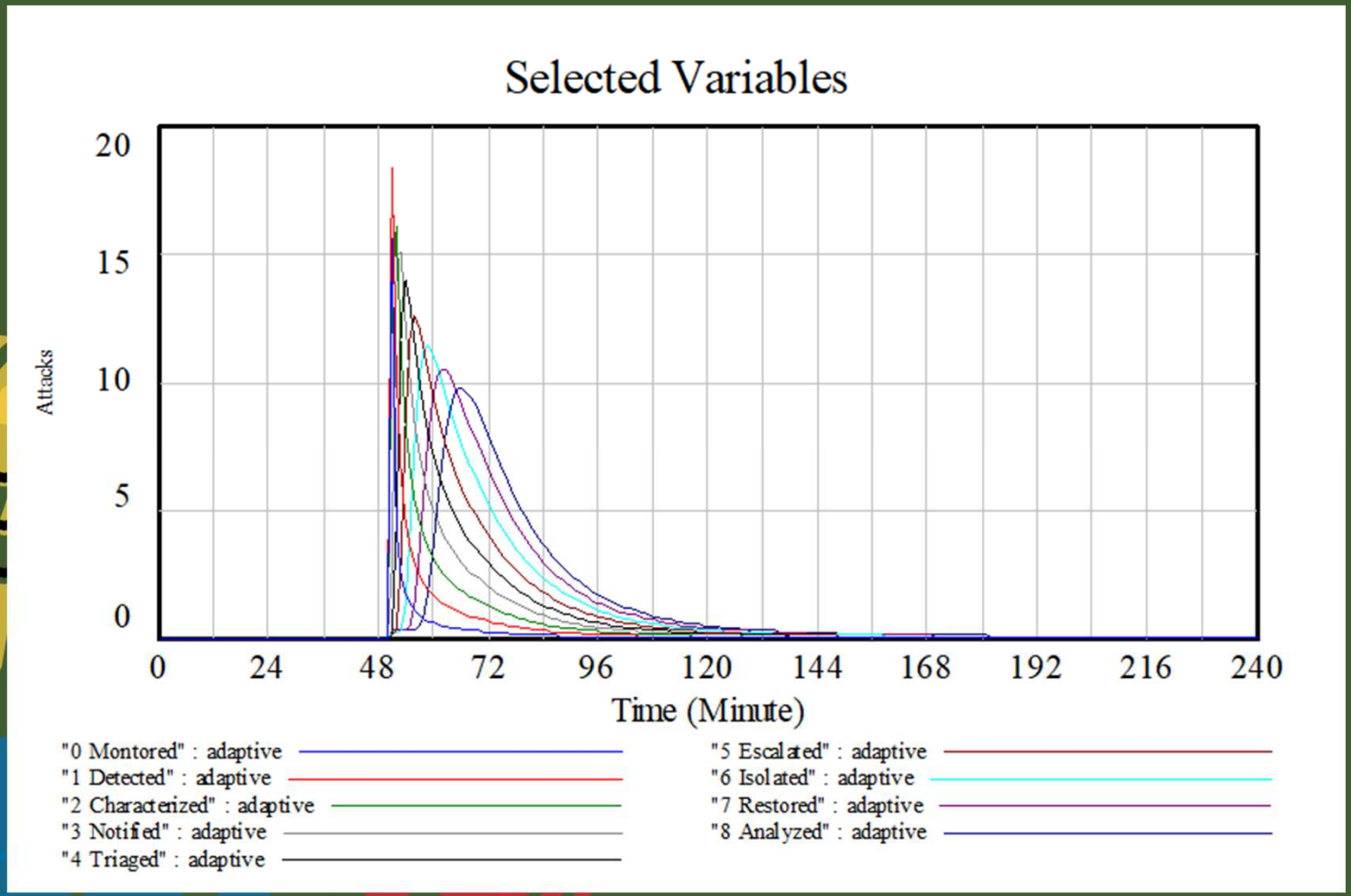
Adaptive

- A fluid allocation where the level of human resources varies based on the level of work at each process

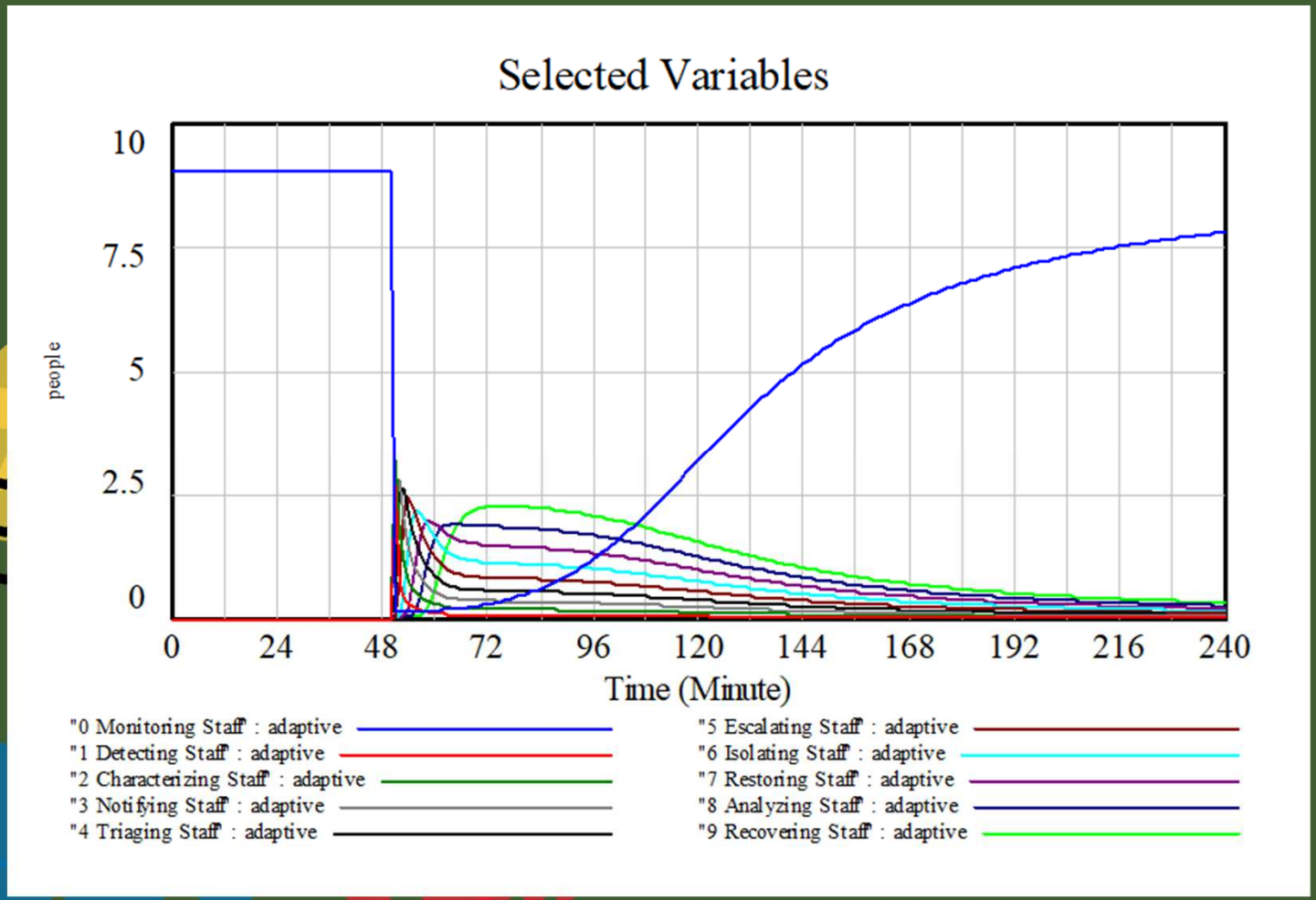
Activity with Balanced Resource Allocation



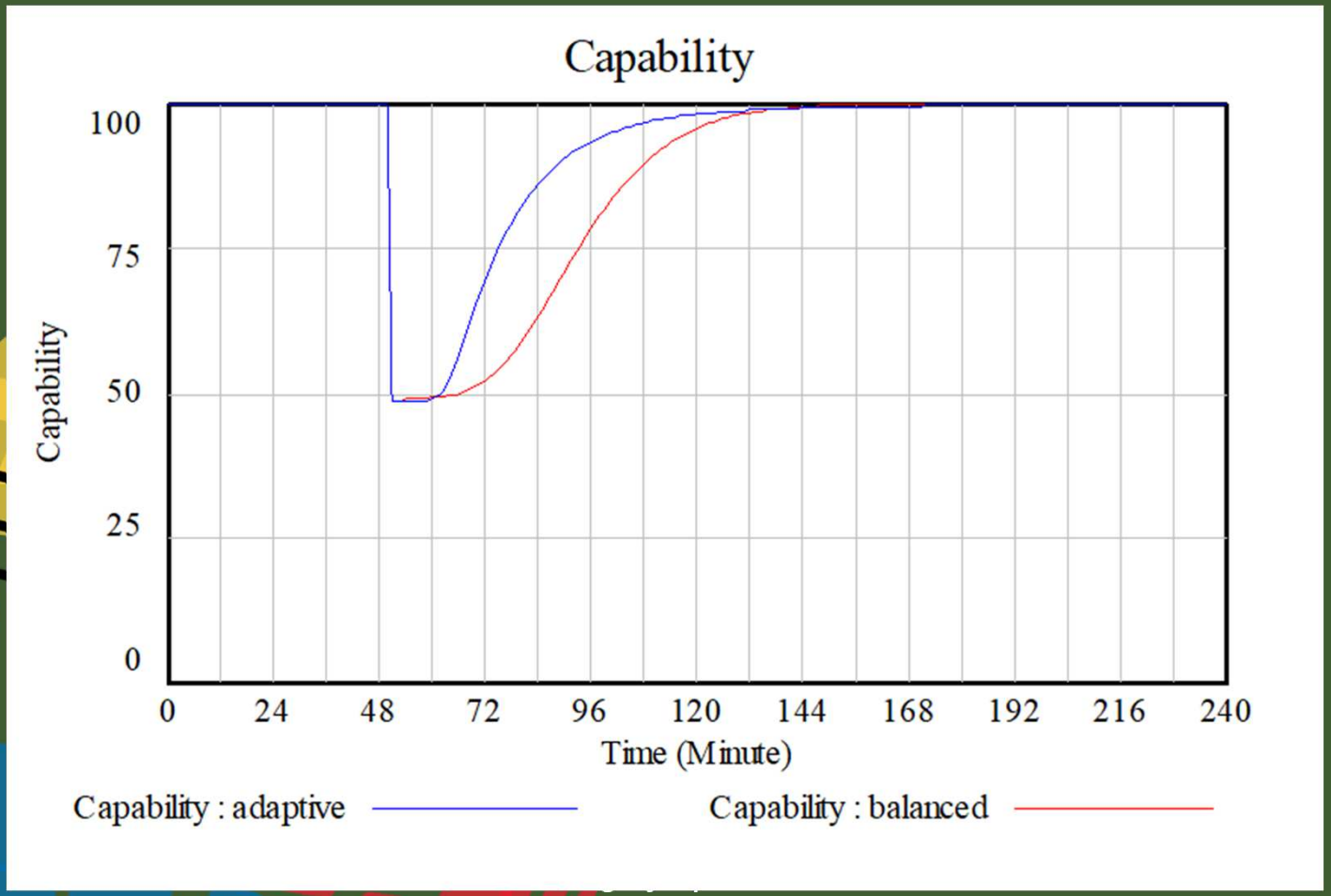
Activity with Adaptive Resource Allocation



Adaptive Assignment of Resources

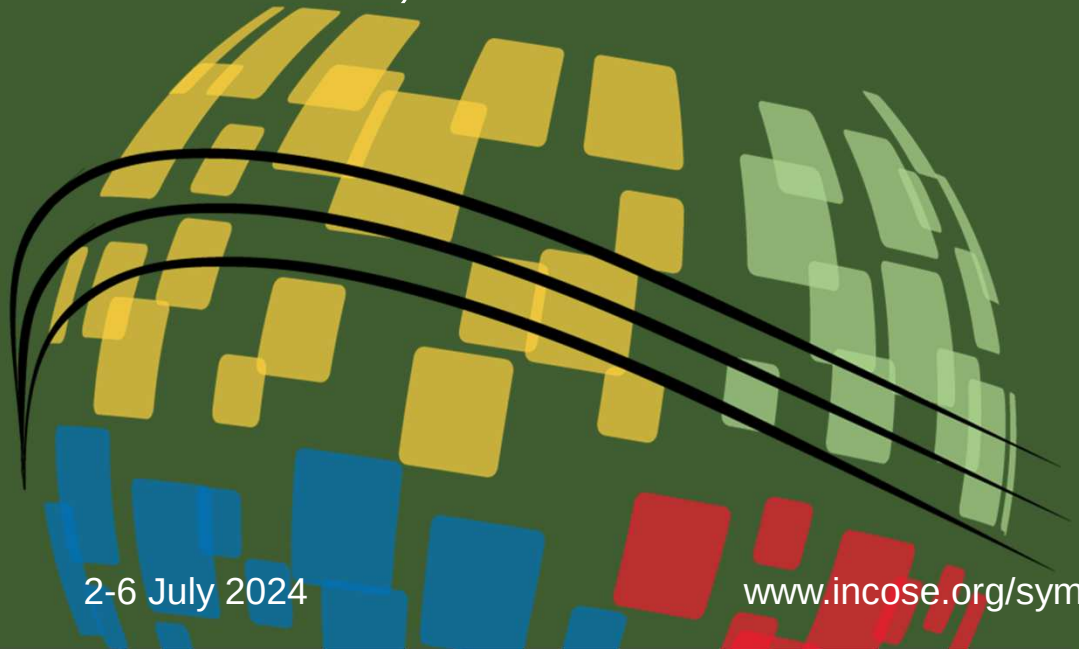


Capability with Balanced and Adaptive Resource Allocations



Discussion

- Adaptive allocation may be
  - *Restores capability at a faster rate,*
  - *By reducing bottlenecks, and*
  - *Flexible, efficient use of resources.*

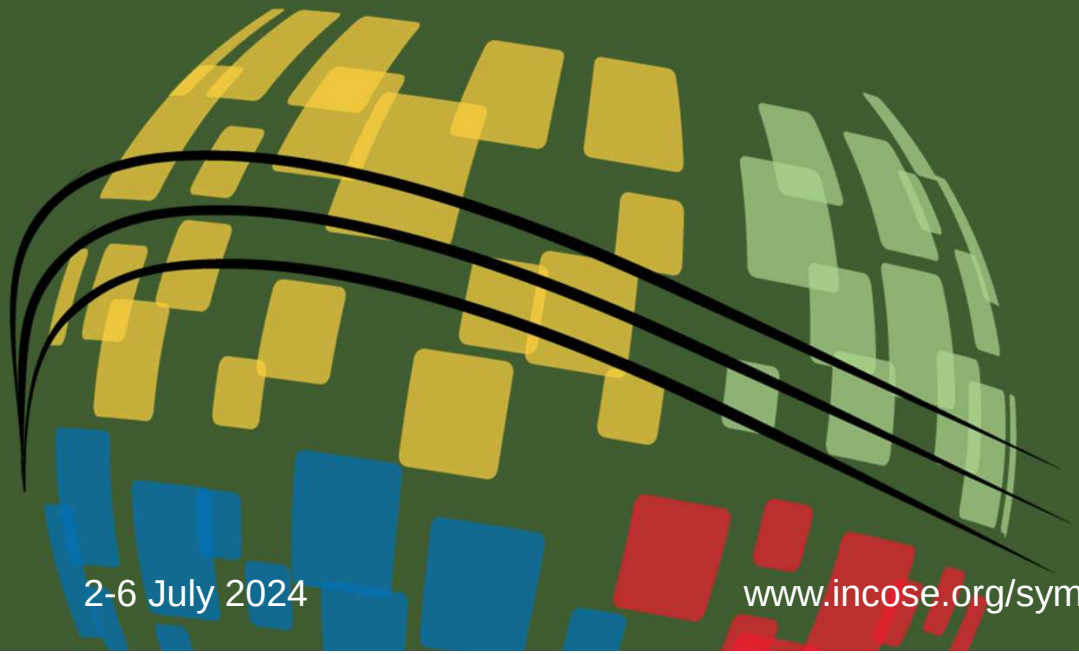


Discussion

- Adaptive allocation may not always be the best strategy
- *Potential drawbacks include*
  - *increased stress,*
  - *burnout,*
  - *turnover,*
  - *mistakes, and*
  - *security breaches*
- *Mitigating measures include*
  - *training,*
  - *support,*
  - *communication*

Key Takeaways

- System Dynamics is valuable for modelling cybersecurity operations.
  - *Provides a holistic understanding of workflow, and*
  - *Enables scenario simulations.*



Key Takeaways

- Adaptive allocation may be more effective than balanced allocation
  - *Flexible and efficient use of human resources,*
  - *Reducing bottlenecks, and*
  - *Improving team effectiveness.*

Key Takeaways

- Unintended consequences of adaptive allocation include
  - *Increased stress and burnout,*
  - *Decreased morale and motivation, and*
  - *Higher risks of errors and security breaches.*

- Organizations should carefully weigh the benefits and drawbacks of adaptive allocation before implementation.

Key Takeaways

- Evaluating the study assumptions thoroughly and continuously is crucial.
  - *Approach's generalizability,*
  - *Simulation model's accuracy, and*
  - *Attack scenarios' representativeness.*

- Further research is needed to validate the findings

You can reach me at any time at ivan.taylor@incose.net

Thank you for listening
Questions and Comments

34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS