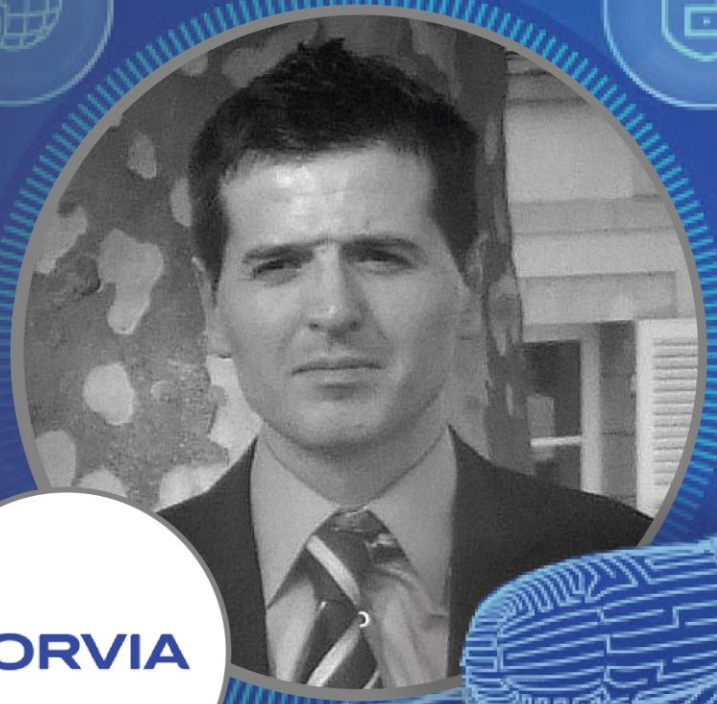
FRANSEC

SECURING FRANCE FROM CYBER THREATS

PRÉSENTATION

AMÉLIORER VOTRE MODÈLE OPÉRATIONNEL DU SOC AVEC UNE APPROCHE SYSTÉMATIQUE

Thomas Billaut, *Head of Cyber Operations*



FORVIA

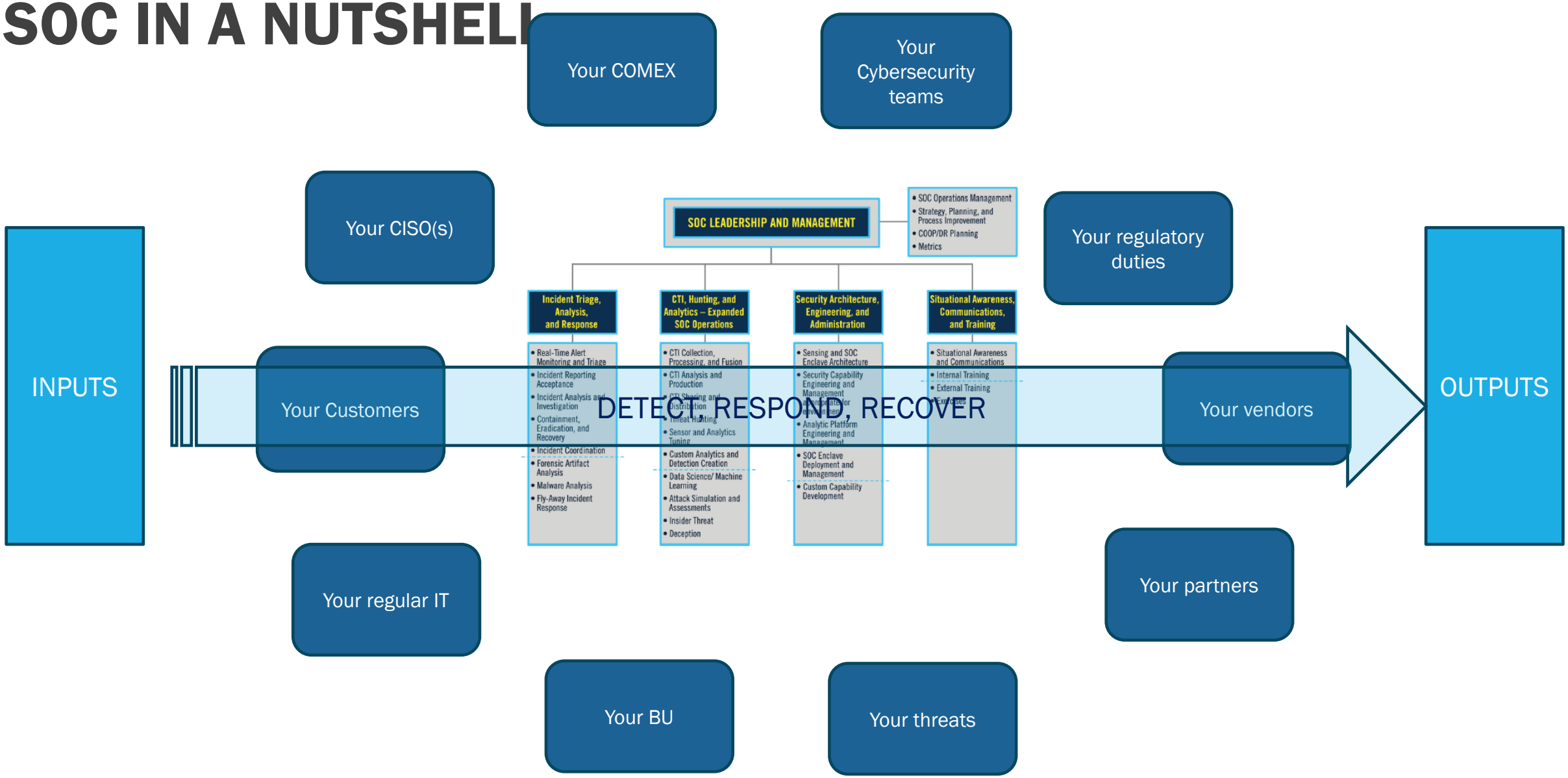
MEMBRE DU COMITÉ D'ORGANISATION

#FRANSEC | PARIS | 10 - 11 SEPTEMBRE 2024

#FRANSEC24

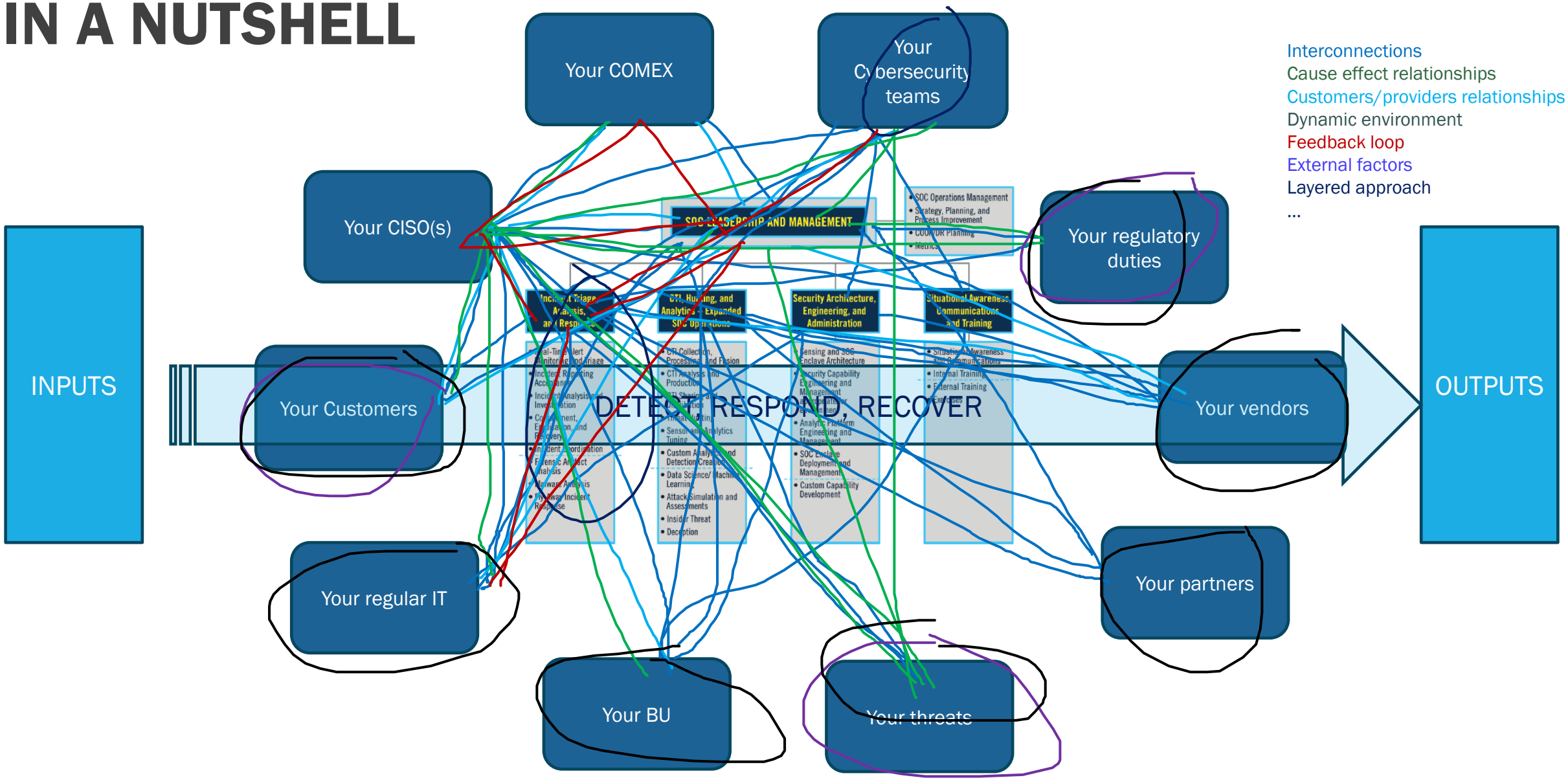
SOC IN A NUTSHELL

SOC IN A NUTSHELL



Source https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center

IN A NUTSHELL



Source https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center

WELCOME TO FRANSEC 2024

$ WHOAMI

@tbillaut

https://fr.linkedin.com/in/thomasbillaut

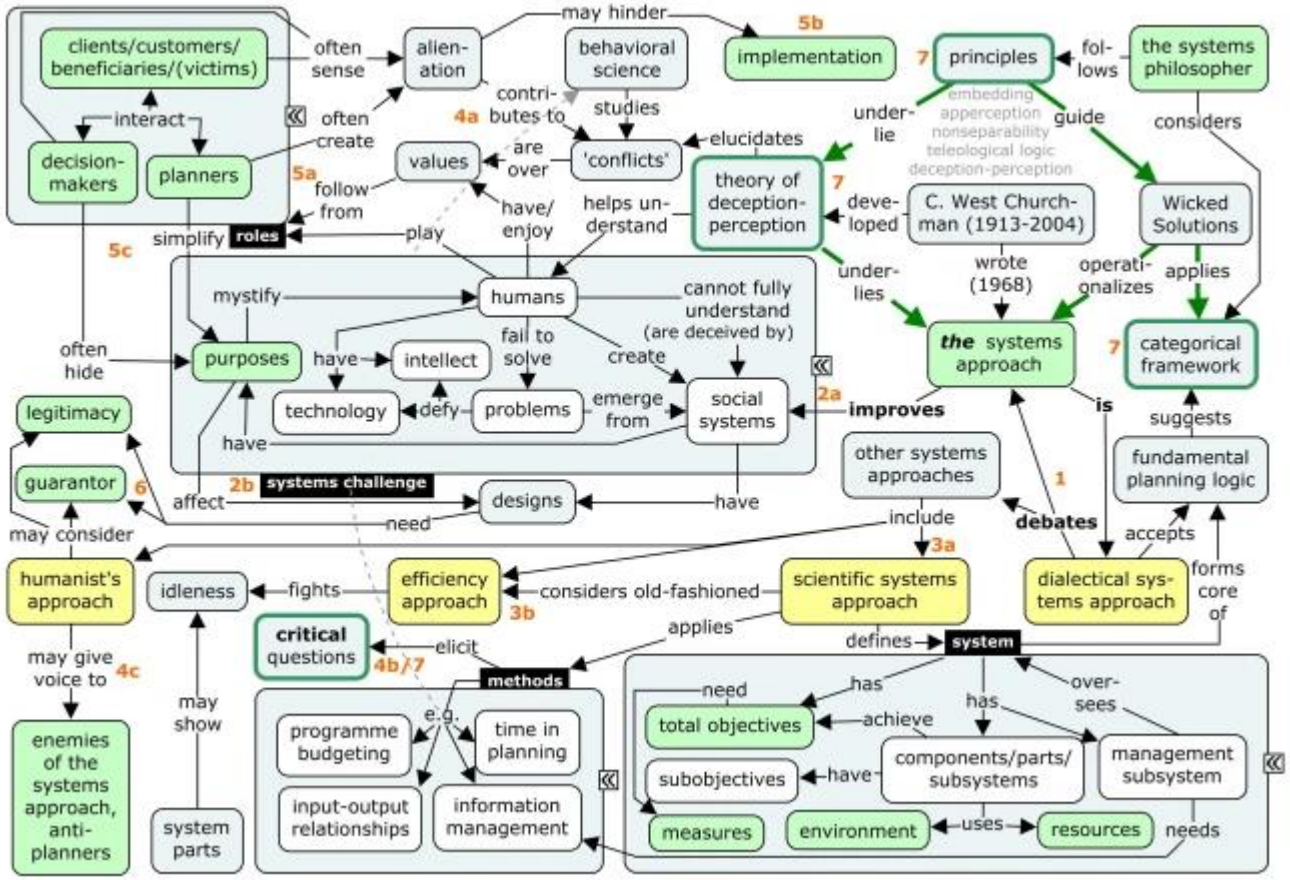
IMPROVE YOUR SOC OPERATING MODEL

WITH SYSTEMIC APPROACH

THOMAS BILLAUT

FRANSEC 2024

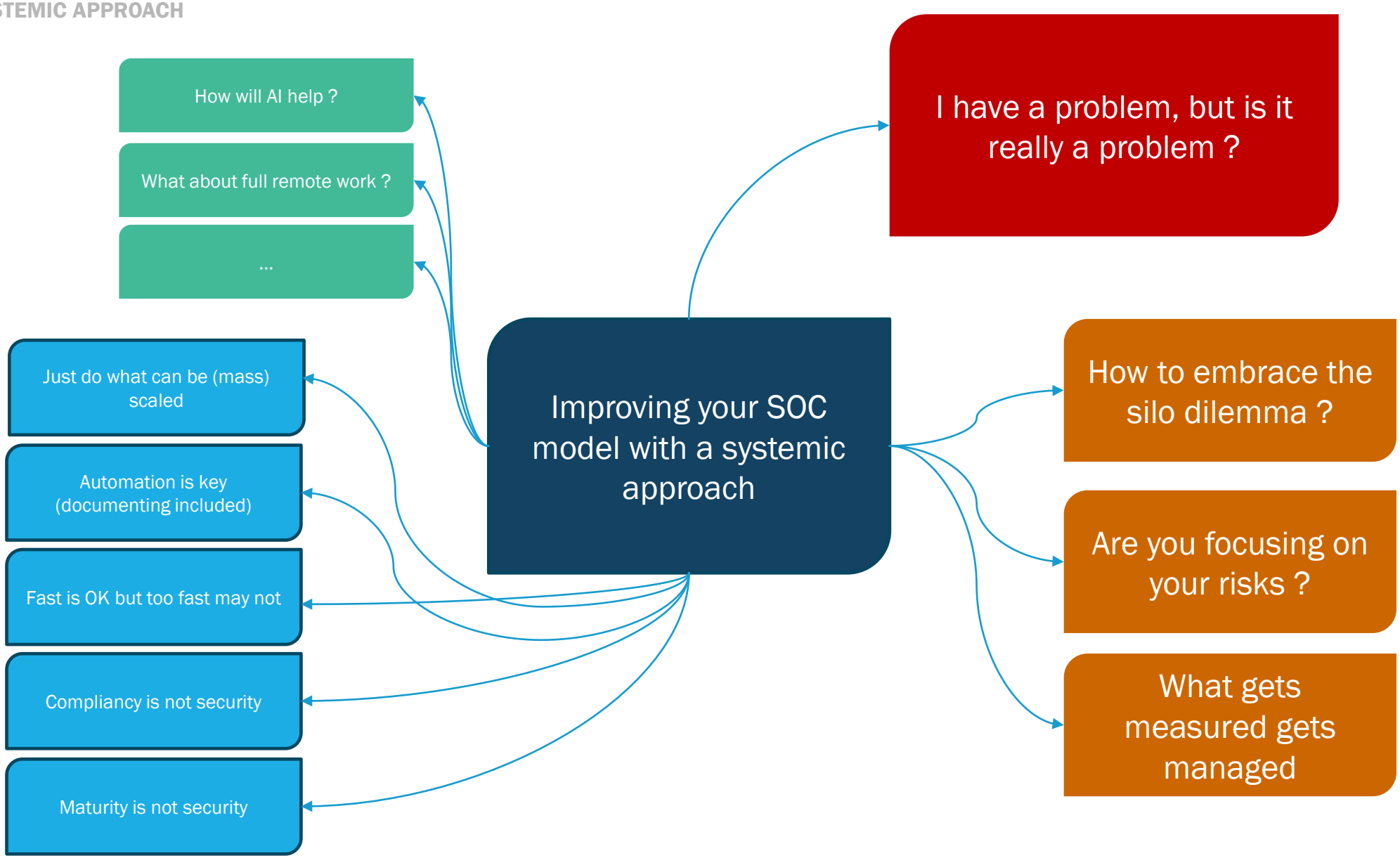
IMPROVE YOUR SOC OPERATING MODEL
WITH SYSTEMIC APPROACH



> THE SYSTEMIC APPROACH IS A WAY TO HANDLE A COMPLEX SYSTEM WITH A GLOBAL POINT OF VIEW AS A LIVING SYSTEM

Source https://csl4d.wordpress.com/2017/07/28/the-origins-of-the-systems-approach-2/
https://systemic-solutions.org/systemic-approach/

IMPROVE YOUR SOC OPERATING MODEL
WITH SYSTEMIC APPROACH



AGENDA

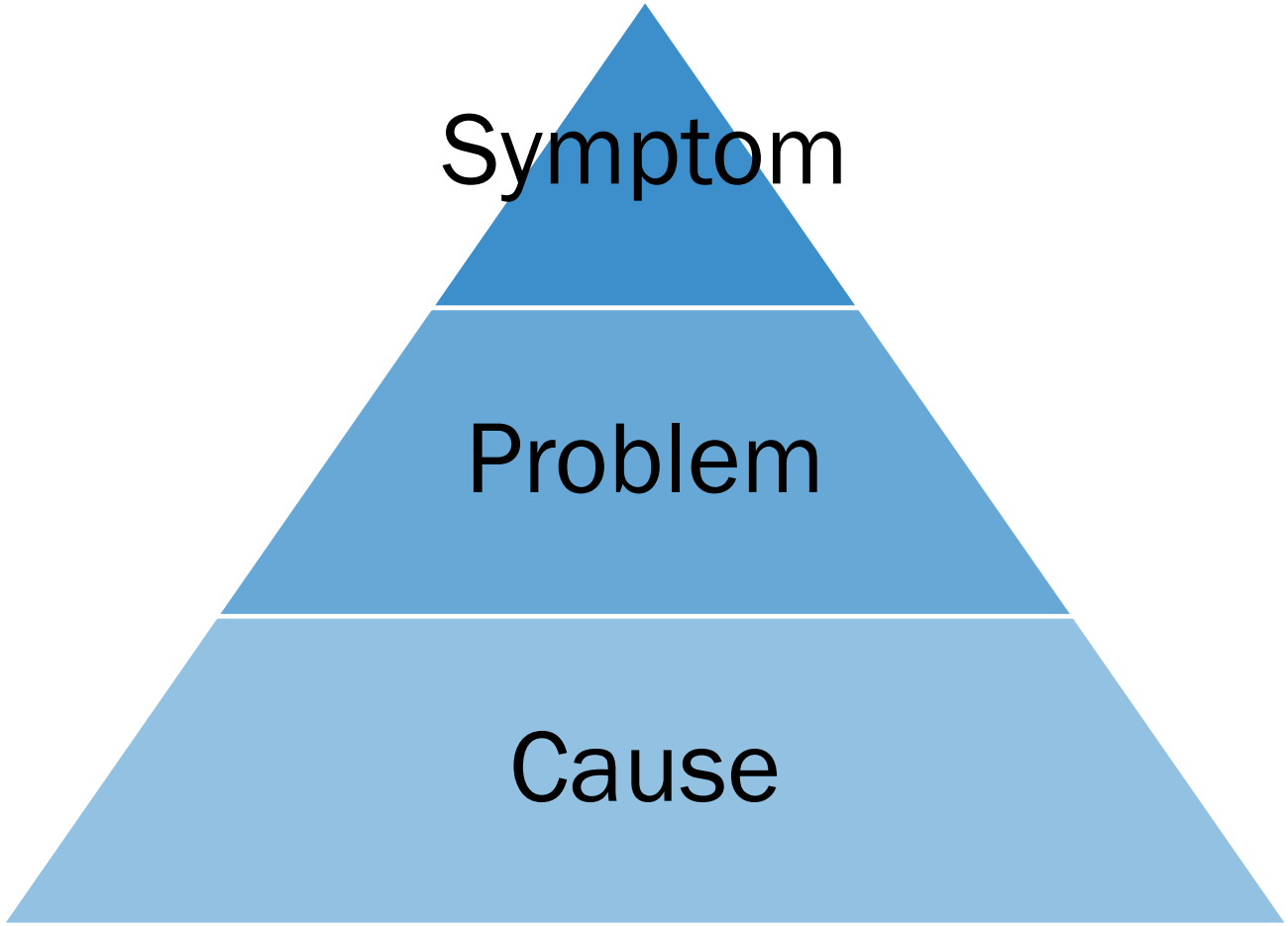
- I have a problem, but is it really a problem ?
- How to embrace the silo dilemma ?
- Are you focusing on your risks ?
- What gets measured gets managed
- Let’s conclude

AGENDA

- I have a problem, but is it really a problem ?
- How to embrace the silo dilemma ?
- Are you focusing on your risks ?
- What gets measured gets managed
- Let’s conclude

IMPROVE YOUR SOC OPERATING MODEL
WITH SYSTEMIC APPROACH

> THE PROBLEM IS NEVER THE PROBLEM. IT IS ONLY A SYMPTOM OF SOMETHING MUCH DEEPER.
>
> VIRGINIA SATIR

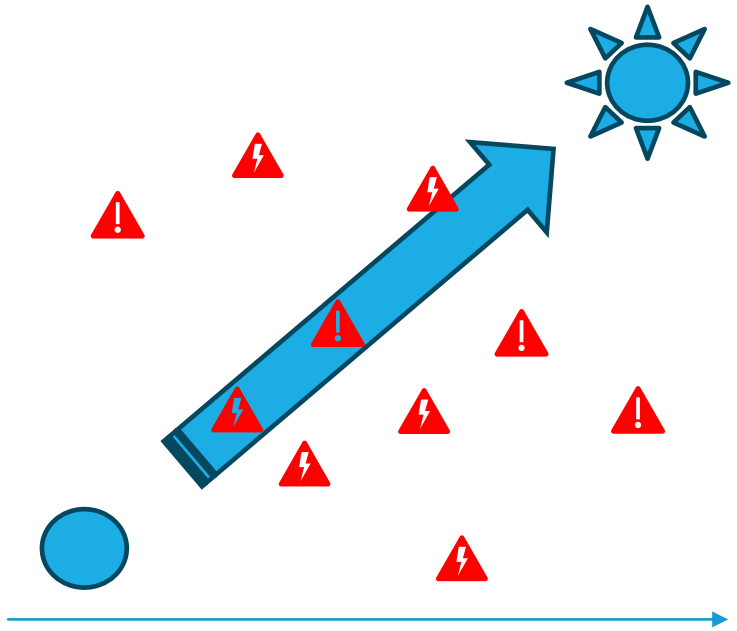


I HAVE A PROBLEM

BUT IS IT REALLY A PROBLEM ?

Changing our perspective on problem (= blockage + desire)

- An organization is a problem-solving machine
  - If you don't manage the problem
- Identifying the Real Problem (for you) is key
  - What is the shining destination ?
    - The Why ?
    - The For What ?
  - Which problems are on the road ?
  - Which problems (in order) need to be tackled ?
    Keep in mind the landscape is dynamically changing when you will modify the system..
  - Symptoms vs. Root Causes: Distinguish between observable issues (symptoms) and underlying problems (possibly up stream)
  - Data Analysis: Use data to identify patterns, trends, and anomalies that point to systemic issues
  - Stakeholder, staff member and customer Interviews: Gather insights from SOC personnel, management, and other relevant stakeholders



I HAVE A PROBLEM

BUT IS IT REALLY A PROBLEM ?

Resolving Issues with a Common System Representation

- System modeling and representation
- **Process Mapping:** Create visual representations of SOC processes to identify bottlenecks, inefficiencies, and potential vulnerabilities.
- **Shared Understanding:** Foster a common understanding of the SOC's operations and goals among all team members.
- **Standardized Procedures:** Implement standardized procedures and guidelines to ensure consistency and efficiency.
- Understanding the Process Flow
  - **Cause-and-Effect Analysis:** Identify how changes in one part of the process impact other areas.
  - **Feedback Loops:** Analyze how feedback mechanisms can improve the system's performance.
  - **Continuous Improvement:** Establish a culture of continuous improvement to address emerging challenges and adapt to changing threats.

I HAVE A PROBLEM

BUT IS IT REALLY A PROBLEM ?

Pay attention to the following thoughts / idea :

- Problem = Solution
- Homeostasis / the scapegoat
- All the known problem solving bias (Confirmation, anchoring, Overconfidence, Groupthink, Abilene paradox, loss aversion, Sunk cost fallacy, etc ...)

Encourage :

- Change perspective / critical thinking
- Diversity
- Do not look for a culprit
- Try to heal the system

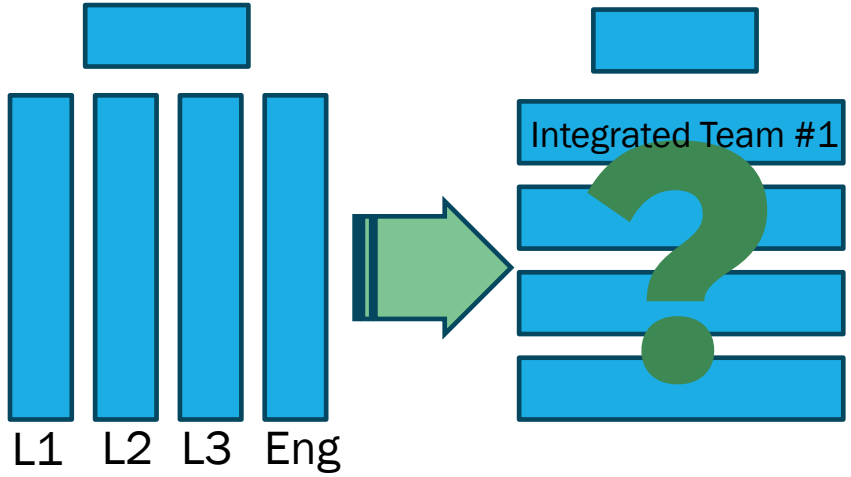
AGENDA

- I have a problem, but is it really a problem ?
- How to embrace the silo dilemma ?
- Are you focusing on your risks ?
- What gets measured gets managed
- Let’s conclude

HOW TO EMBRACE THE SILOS DILEMMA

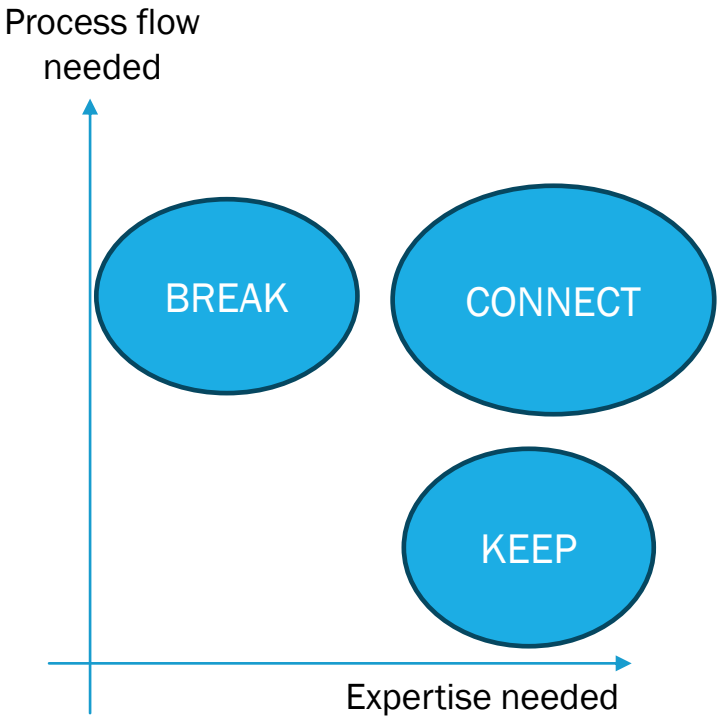
DO YOU REALLY WANT TO BREAK THEM ? OR DO YOU RATHER WANT TO CONNECT THEM ?

- In a nutshell, SOC are facing the same challenges than every business
  - How to do more and better (with less) ?
  - How to do fast ?
- Automation and AI can be both seen as means and reinforcement causes for this need for speed and disintermediation
- In order to accelerate, breaking silo brings to reduce the number of interfaces which is usually a good guess to reduce the toll and accelerate dedicated process flow
- However
  - it is “one size fits all” solution ?
  - Is it really better to go from vertical silos to horizontal ones ?
  - When do you need silos – and you should keep it ?
  - How to accelerate with silos in my org ?



HOW TO EMBRACE THE SILOS DILEMMA

DO YOU REALLY WANT TO BREAK THEM ? OR DO YOU RATHER WANT TO CONNECT THEM ?



Big picture keys to tackle the problematic :

- Evaluate – ideally periodically – your need for expertise
- Silo is key to create, stimulate and keep expertise
  - *If you don't need deep expertise, challenge the need for silos ;)*
- Silo is slowing down the end2end process
- SOC process usually needs both : speed, flow but deep expertise
- Hybrid approach - or silo connections – seems in this case a far better solution

HOW TO EMBRACE THE SILOS DILEMMA

DO YOU REALLY WANT TO BREAK THEM ? OR DO YOU RATHER WANT TO CONNECT THEM ?

More concreate solutions to make it happen :

- Centralized SOC Governance : make the governance clear for every SOC staff member (everyone has the same representation of the system)
  - SOC office, clear roles and responsibilities, framework
- Enhanced Communication and Collaboration (everyone understands the value brought by each other) : how to bring transparency
  - Regular Meetings and Forums, Collaboration Tools, Cross-Functional Training, …
  - Data Sharing, consumption and Integration
  - Threat intel sharing : might be both strategic, tactical and operational, regular briefing, spontaneous volunteering for working group, …
- Have and contribute to the same objective : Performance Metrics and Key Performance Indicators (KPIs)

AGENDA

- I have a problem, but is it really a problem ?
- How to embrace the silo dilemma ?
- Are you focusing on your risks ?
- What gets measured gets managed
- Let’s conclude

ARE YOU FOCUSING ON YOUR RISKS (AS A SOC) ?

CLASSICAL SYMPTOMS

- Typical symptoms (and not problem) :
  - The SOC is not well organized
  - The SOC is inefficient
  - The SOC governance is not clear
  - The SOC is not skilled in running project
  - The SOC is definitely not supporting the business…
- Typical symptoms (and not problem) diagnosis
  - the symptom (and not the problem) shows up at SOC level
  - but it usually arises upstream with BUs that own their risks (Business Units) and managements (C-level, CISO, org dependants,…)
- When priorisation is not clear : how to prioritize your workstream, your resources ? How to prioritize UCs ? How to prioritize monitoring area? How to assign a severity ?
- A traditional problem => solution approach does not allow you to bring improvements

ARE YOU FOCUSING ON YOUR RISKS (AS A SOC) ?

EMBRACE A SYSTEMIC APPROACH

- Align your SOC org on the risk assessment and periodisation
  - If not available, help while starting small and thinking big
- Can be challenging :
  - need to be worked with business and mgmt.
  - Alignment and priorisation between BU usually challenging
  - Management sponsorships should help
- The SOC is one piece of your security posture in your cyber org
- And Do remember :
  - People only complains when things go wrong
  - if your SOC is so efficient, that’s just normal for most people, no one will congratulate

AGENDA

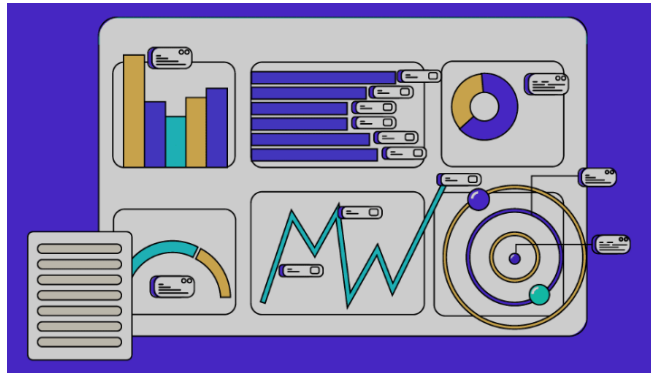
- I have a problem, but is it really a problem ?
- How to embrace the silo dilemma ?
- Are you focusing on your risks ?
- What gets measured gets managed
- Let’s conclude

WHAT GETS MEASURED GETS MANAGED

- Symptoms
  - Too many KPIs : your dashboard kill the actionability and overwhelm rather than inform
  - No relevant KPIs : your mission and your challenges are not clear
  - 1 Dashboard all you can eat for all (staff, sec mgmt., mgmt., business)
  - No KPI : (
- Consequences / impact ?
  - How do you measure your success ?
  - What are your (SMART) objectives ?
  - How do you measure the completion ?
  - How do you create motivation not putting your SOC into the hamster wheel…
- The key to an actionable SOC dashboard is to focus on the most meaningful metrics that provide a clear picture of performance and security posture

WHAT GETS MEASURED GETS MANAGED

- What is your mission (people, process, tech) ?
- What are your current challenges ?
- What are you currently improving ?



Your (current) dashboard

WHAT GETS MEASURED GETS MANAGED

WHAT MAKES A GOOD KPI ?

1. Relevance
   - Alignment with Goals and objectives (time framed
   - Business Impact
2. Actionability
   - Clear Decision-Making
   - Specificity
3. Measurability
   - Quantifiable
   - Data Availability
4. Timeliness
   - Real-Time Insights
   - Trend Analysis
5. Simplicity
   - Clarity
   - Conciseness
6. Comparability
   - Benchmarking
   - Contextual Relevance

WHAT GETS MEASURED GETS MANAGED

TIPS

- Your SOAR can be your best ally for some metrics (completely automated) :
  - nb of alerts
  - nb of incident (with distribution : compliance malicious, FP)
  - nb of most severe incident
  - nb of crisis / pre crisis mode
  - Incident Detection Rate (nb total of incidents + nb of most severe incidents)
  - Mean Time to Detect (MTTD)
  - Mean Time to Respond (MTTR
  - False Positive Rate: The percentage of alerts that were incorrectly flagged as malicious

- OKR (Objective Key Results) can bring a precious help on workstream and (improvements) project

AGENDA

- I have a problem, but is it really a problem ?
- How to embrace the silo dilemma ?
- Are you focusing on your risks ?
- What gets measured gets managed !
- Let’s conclude

CONCLUSION

- Consider the SOC as a complex system
- Change your perspective on problem (= blocage + desire) that can be « just » a symptom
- Cyber technics are necessary but far from enough for running a SOC
- Start small (and start somewhere !) but think big
- Stay optimistic : the most important is the journey, not the destination :)

“WITH ORDINARY TALENT AND EXTRAORDINARY PERSEVERANCE, ALL THINGS ARE ATTAINABLE

THOMAS FOXWELL BUXTON

THANK YOU / MERCI

SHOULD YOU WANT TO DISCUSS FURTHER, DO NOT HESITATE TO CONTACT ME

@tbillaut

https://fr.linkedin.com/in/thomasbillaut