CENSUS
IT Security Works

Digital Ship Athens Spring Conf 2023

Be the captain in a cyber security budget discussion

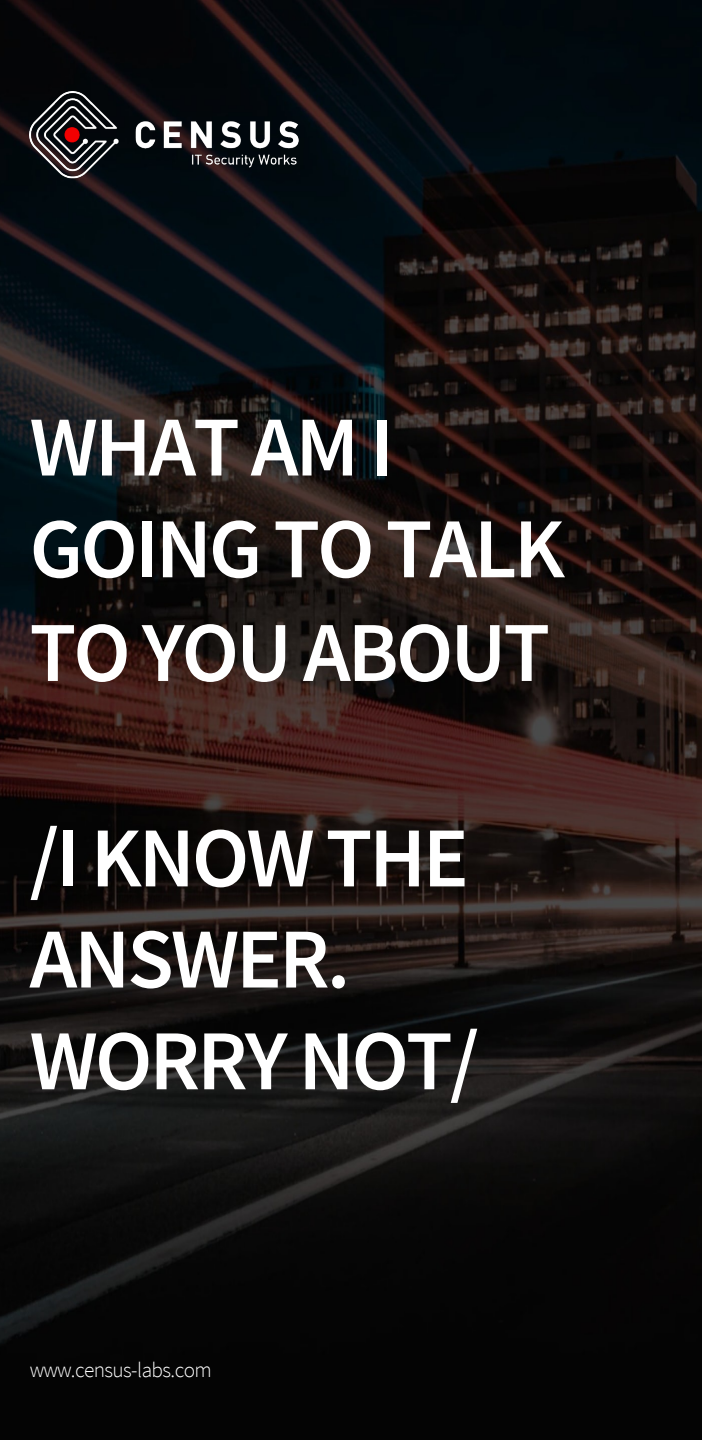
Chara Vassiliadou
chvassiliadou@census-labs.com

CENSUS
IT Security Works

WHO AM I?

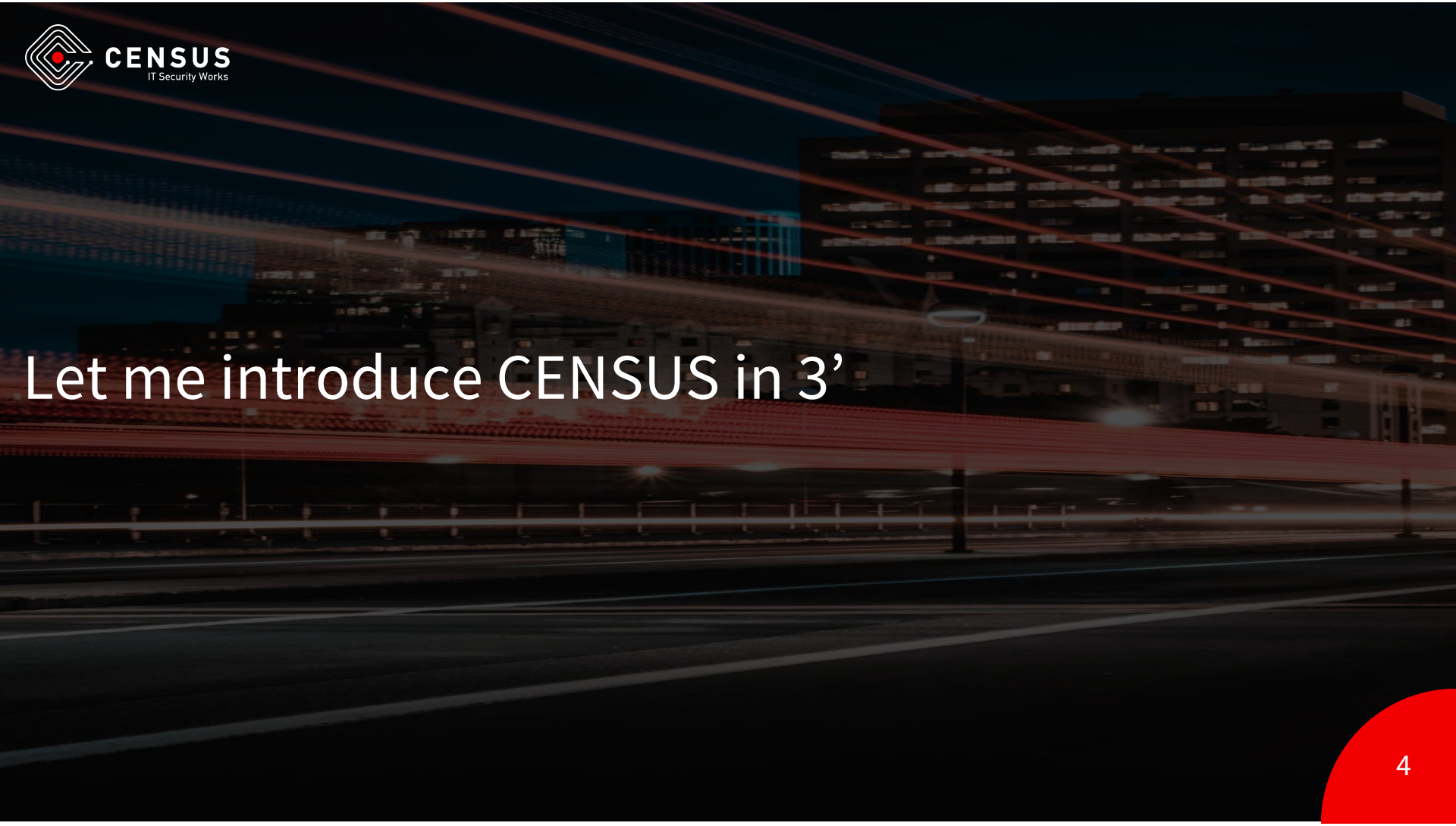
/THIS IS NOT AN EXISTENTIAL QUESTION/

- Name: Chara Vassiliadou
- Background: Computer Engineer with MS in Cyber Security
- Current Role: Commercial Director
- Some Previous Roles: Information Security Manager, Product Manager of IT Sec Solutions
- Working in this sector since 2006
- Still, I know nothing. Just like John Snow



Agenda

- Let me introduce CENSUS in 3’
- What is Cybersecurity (I know you all know)
- What is ROI… Baby don’t hurt me
- The good, the bad and the ugly of security investments
- And now what?
- Questions and possible Answers


CENSUS
IT Security Works
Let me introduce CENSUS in 3’

CENSUS
IT Security Works

CENSUS at a glance

- **CENSUS** is an **internationally acclaimed** Cybersecurity services provider, supporting the needs of **multiple industries**.
- We are offering state-of-the-art services to organizations **worldwide** to cover the complex needs of today's **IT & OT ecosystems**:
  - Organisation Security
  - Product Security Assessments
  - Secure Systems Development Lifecycle
  - Vulnerability Research
  - Information Security Consulting
- Services built upon the **company's leading research** to provide high quality InfoSec services.
- We are very proud of our **ethos**, as we care about **quality (in) systems**.

65 Security engineers

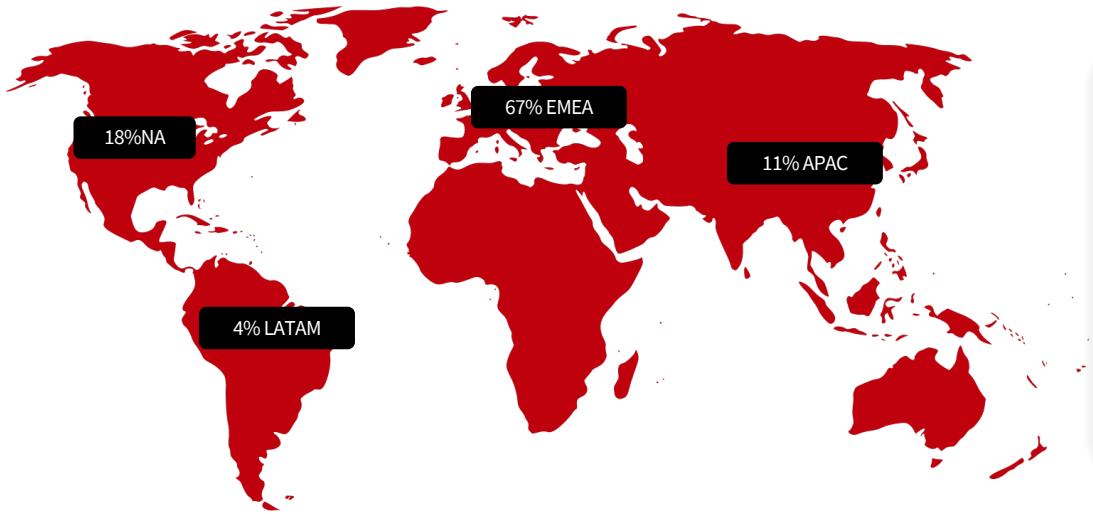
12+ Years of innovation

Company certified for quality and security management systems

CENSUS at a glance

Global presence

We help clients with their cybersecurity maturity journey by providing end to end state of the art assessment of their security posture to improve their cyber resilience and leverage the benefits of digital transformation.



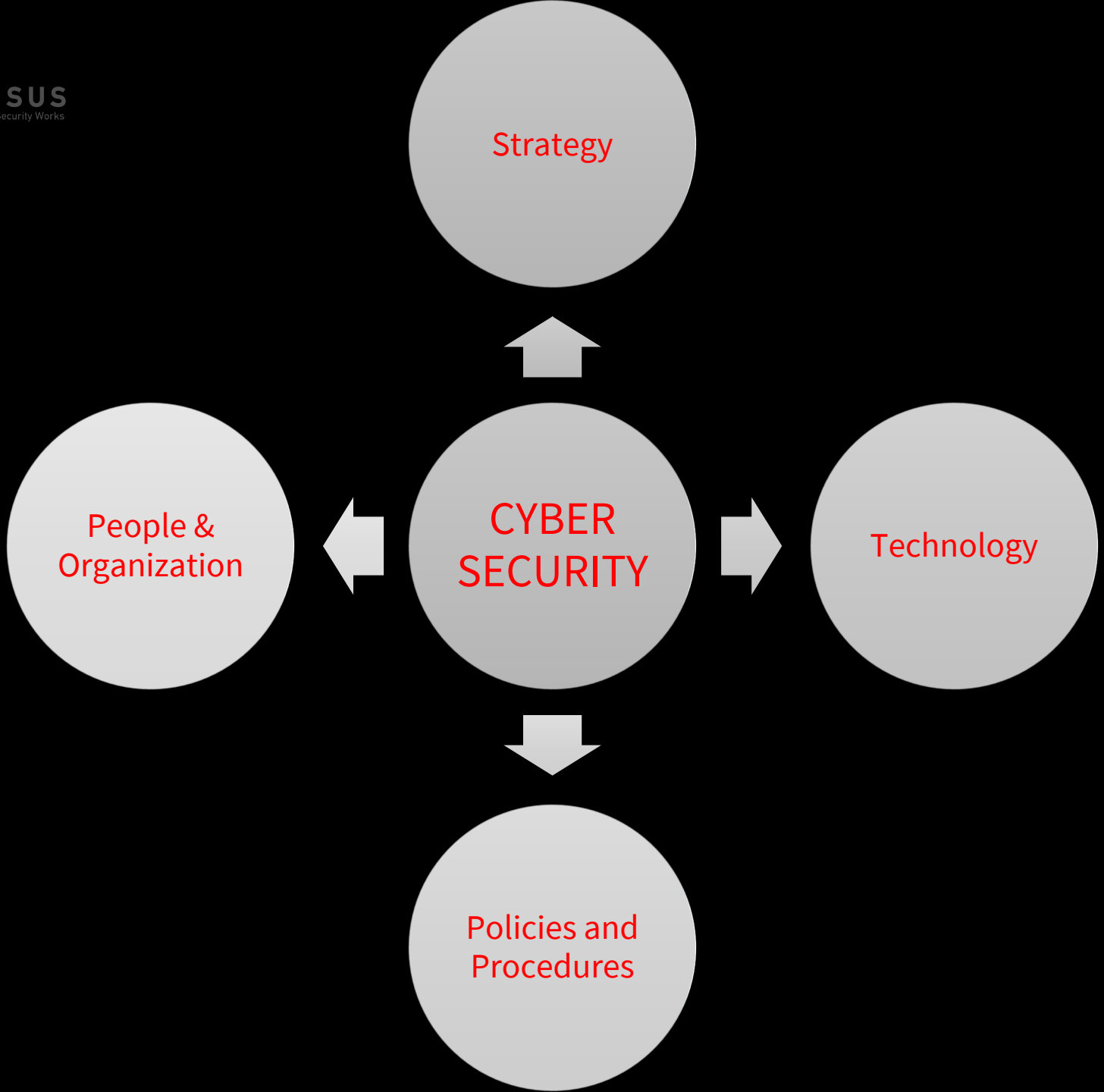
19+
Countries

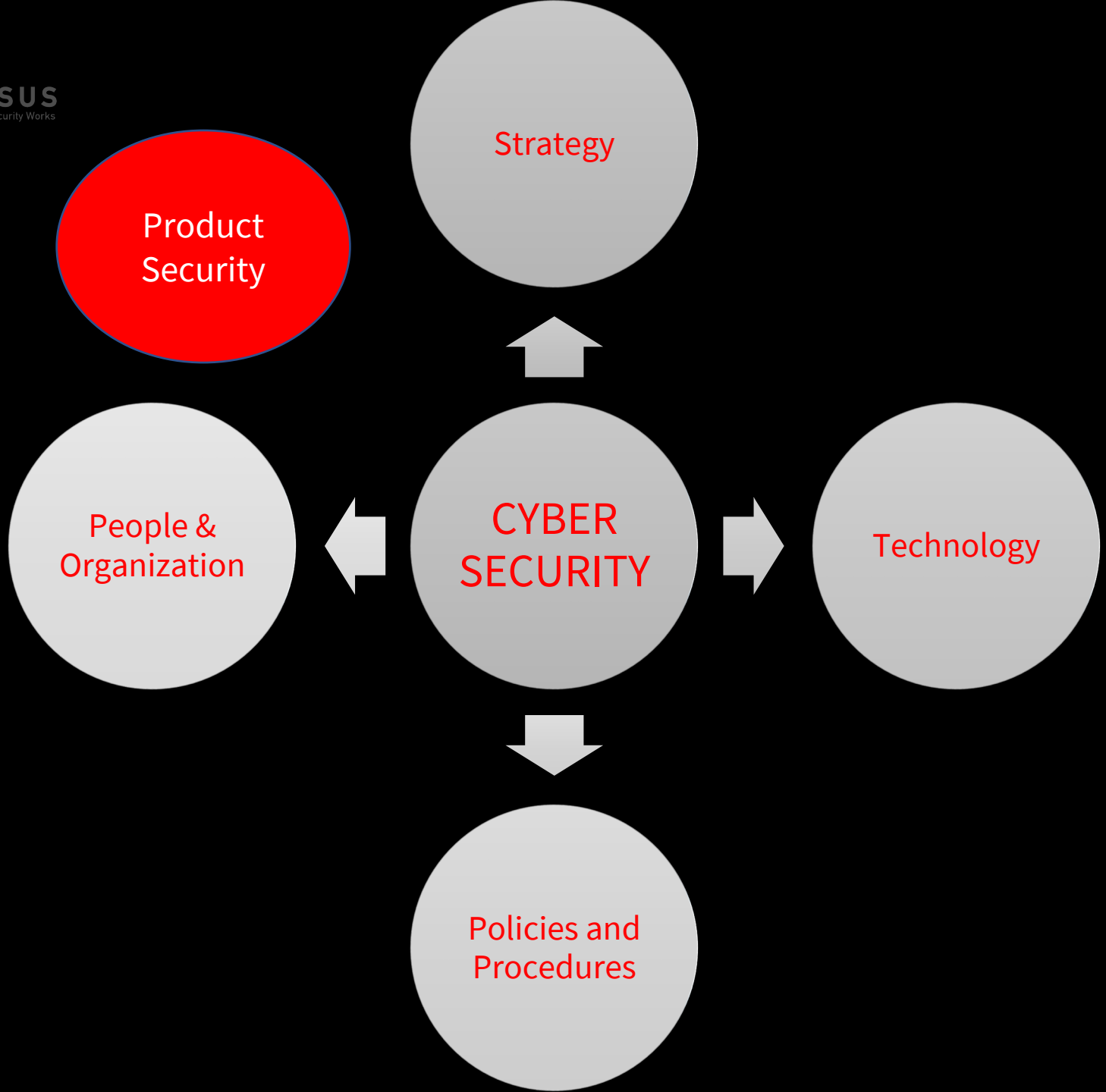
~400
Clients
80+ Fortune 500

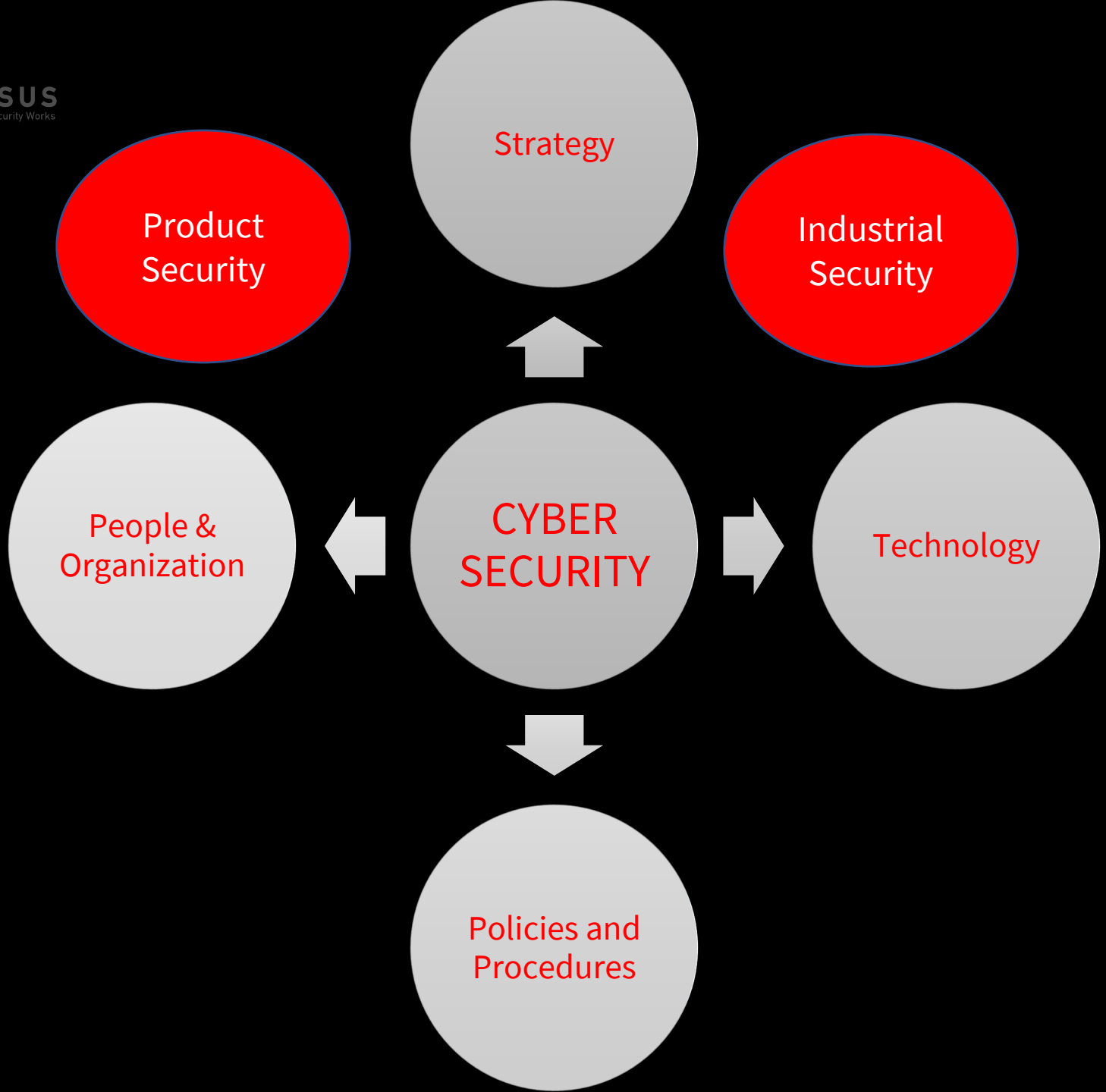
In multiple market sectors

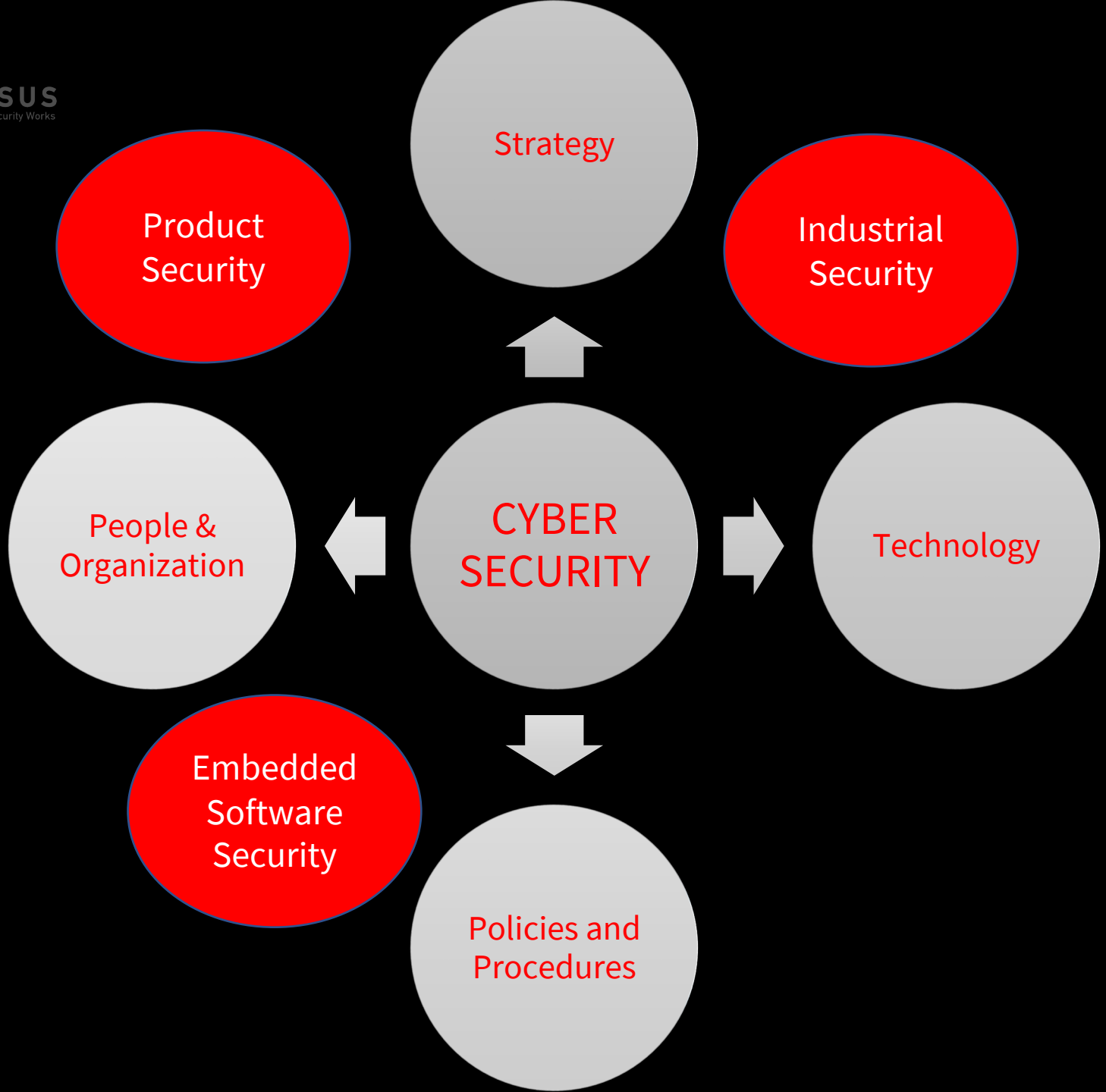
- Aerospace & Defence§
- Government
- Healthcare
- Maritime
- Transportation
- Banking, Finance & Insurance
- Industrial & Internet of Things
- Energy & Utilities
- Software Companies
- Application Developpers

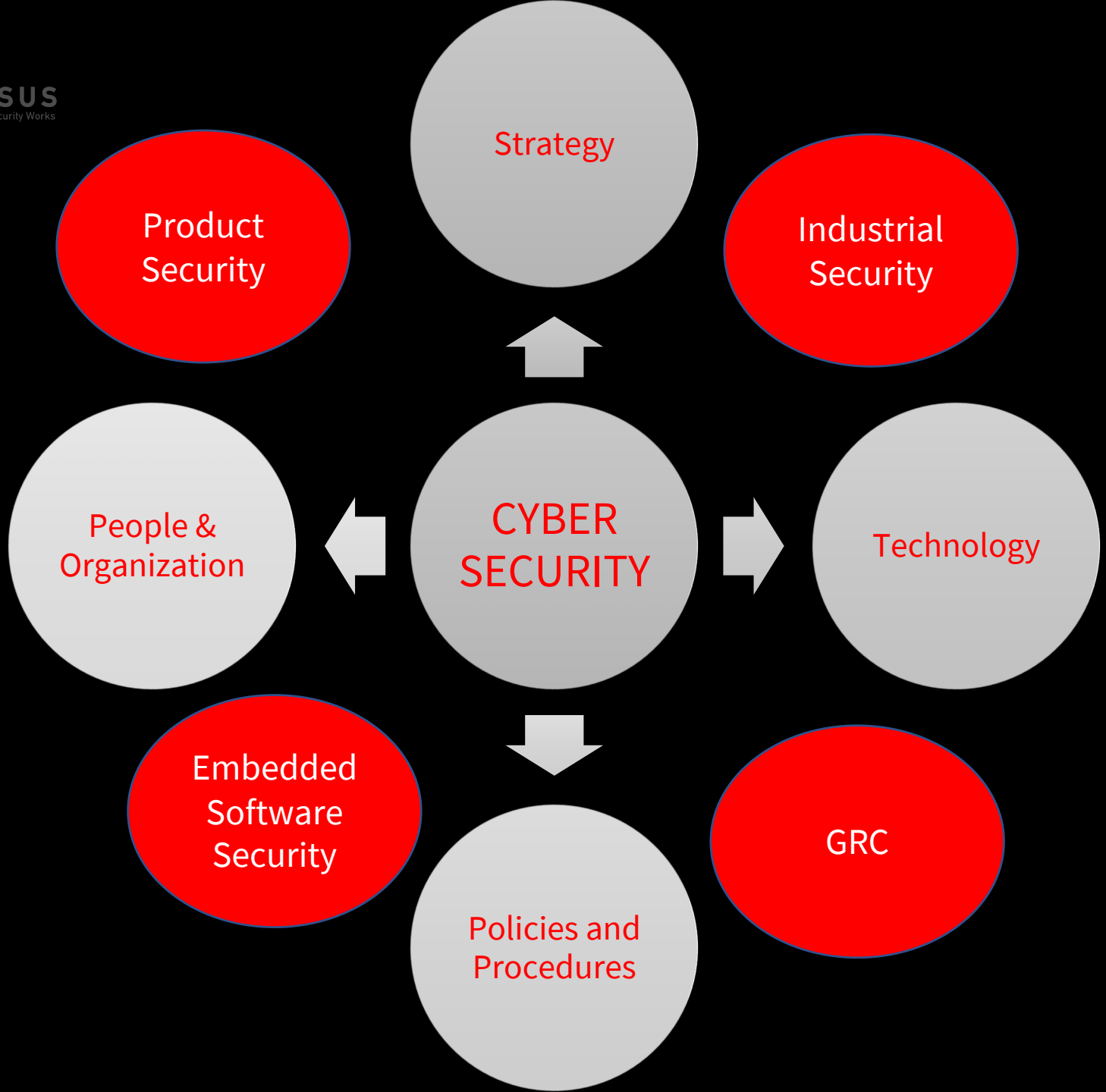
What is Cybersecurity (I know you all know)

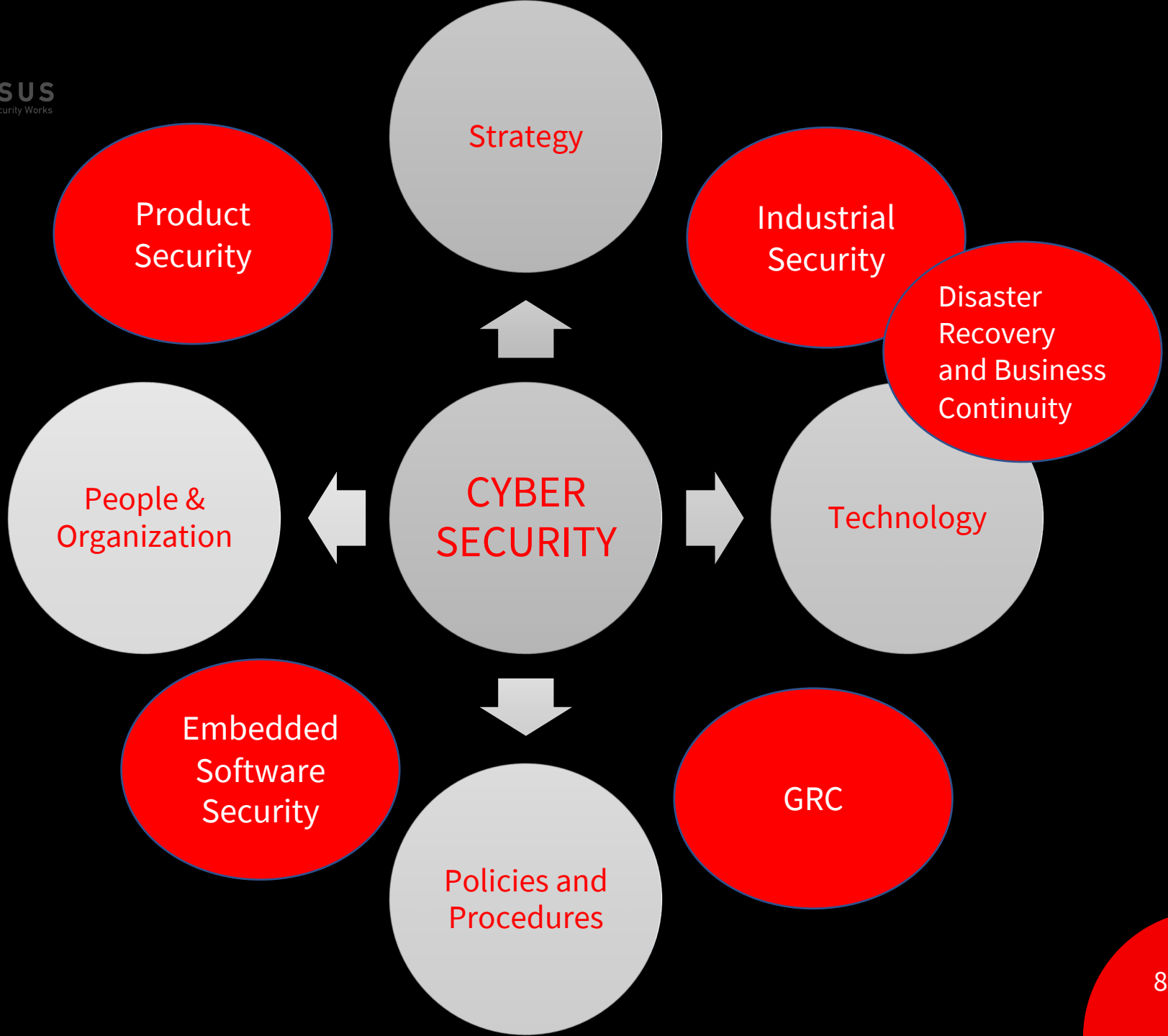

Strategy
People &
Organization
CYBER
SECURITY
Technology
Policies and
Procedures

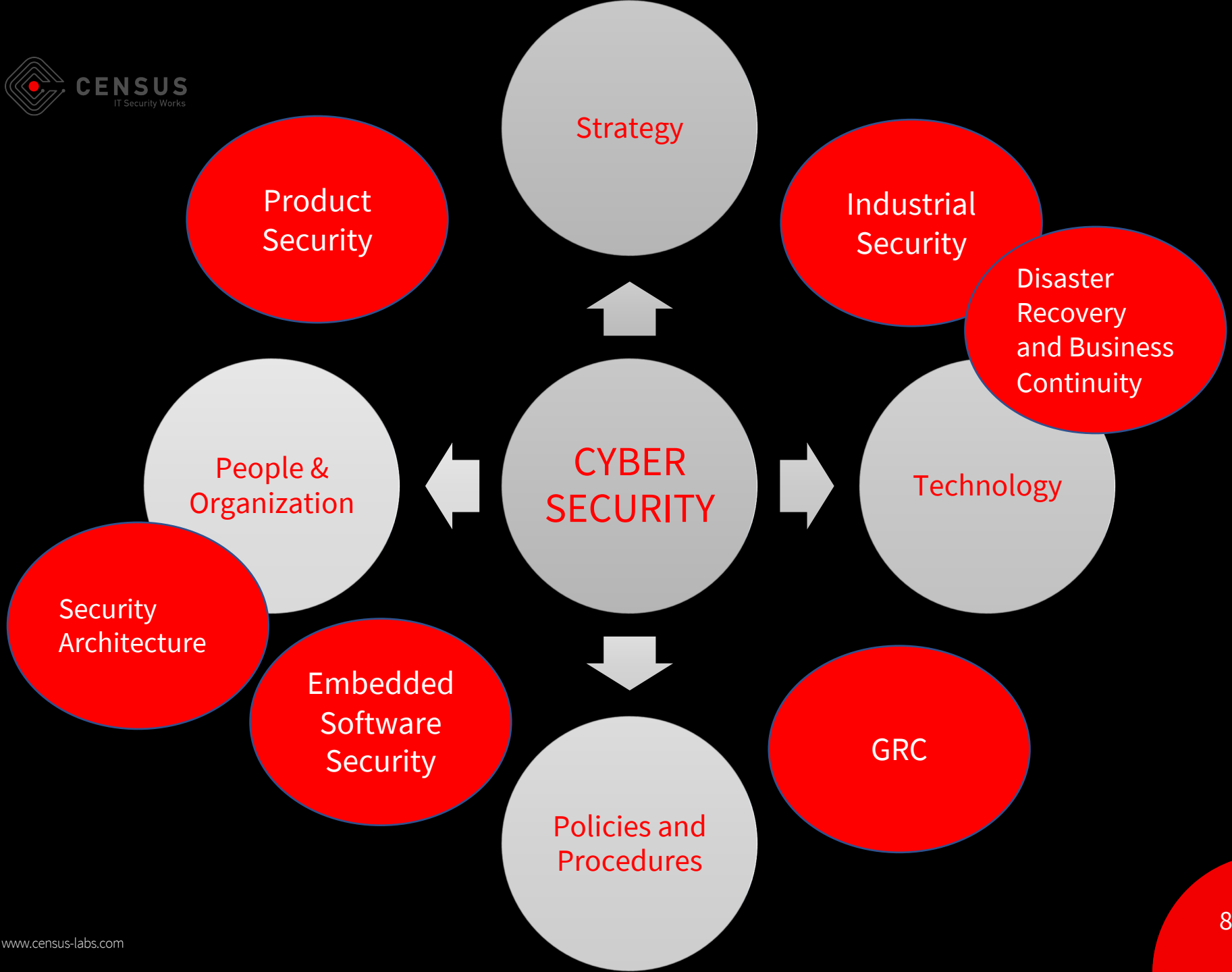

Strategy
Product Security
People & Organization
CYBER SECURITY
Technology
Policies and Procedures

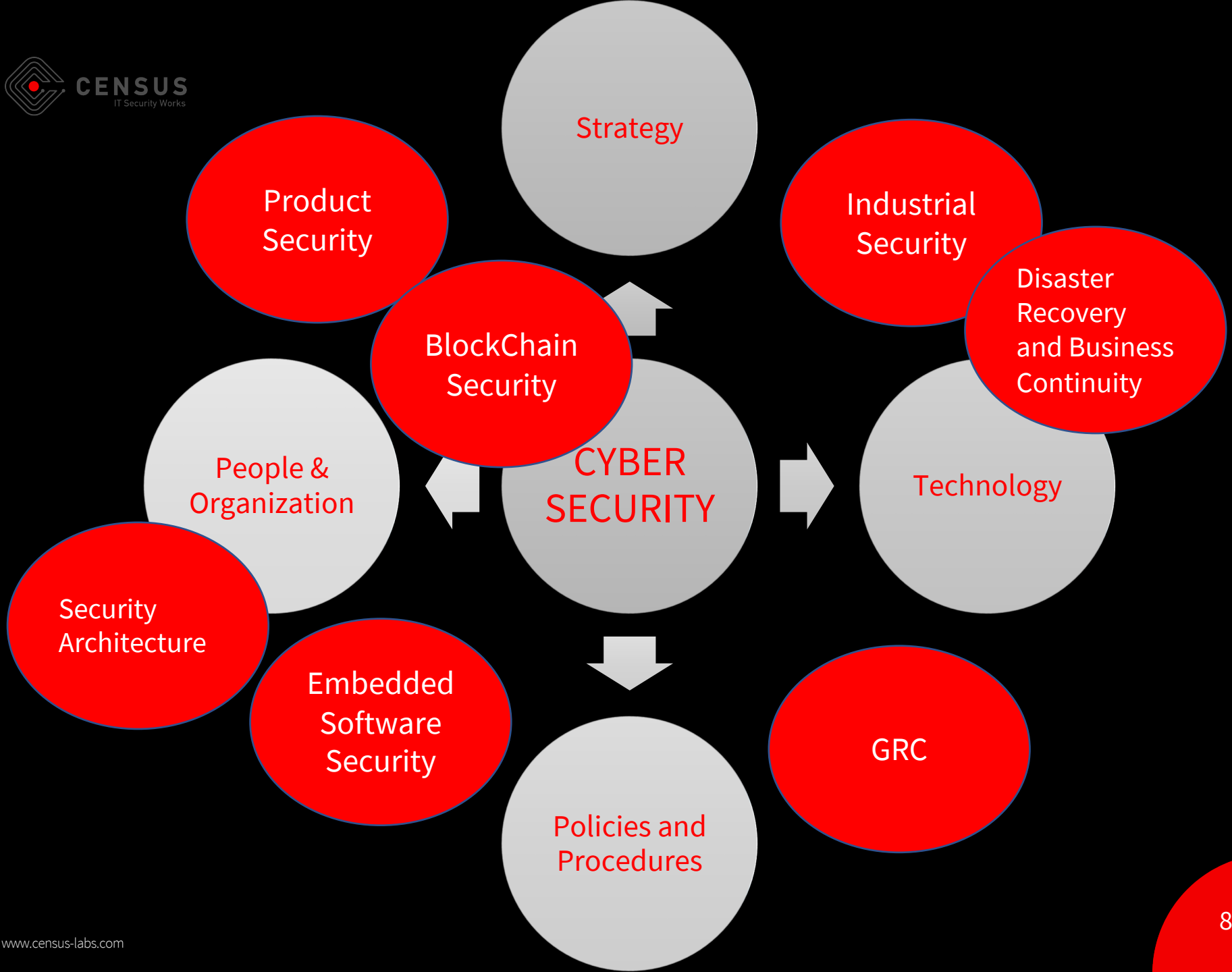

Strategy
Product Security
Industrial Security
People & Organization
CYBER SECURITY
Technology
Policies and Procedures

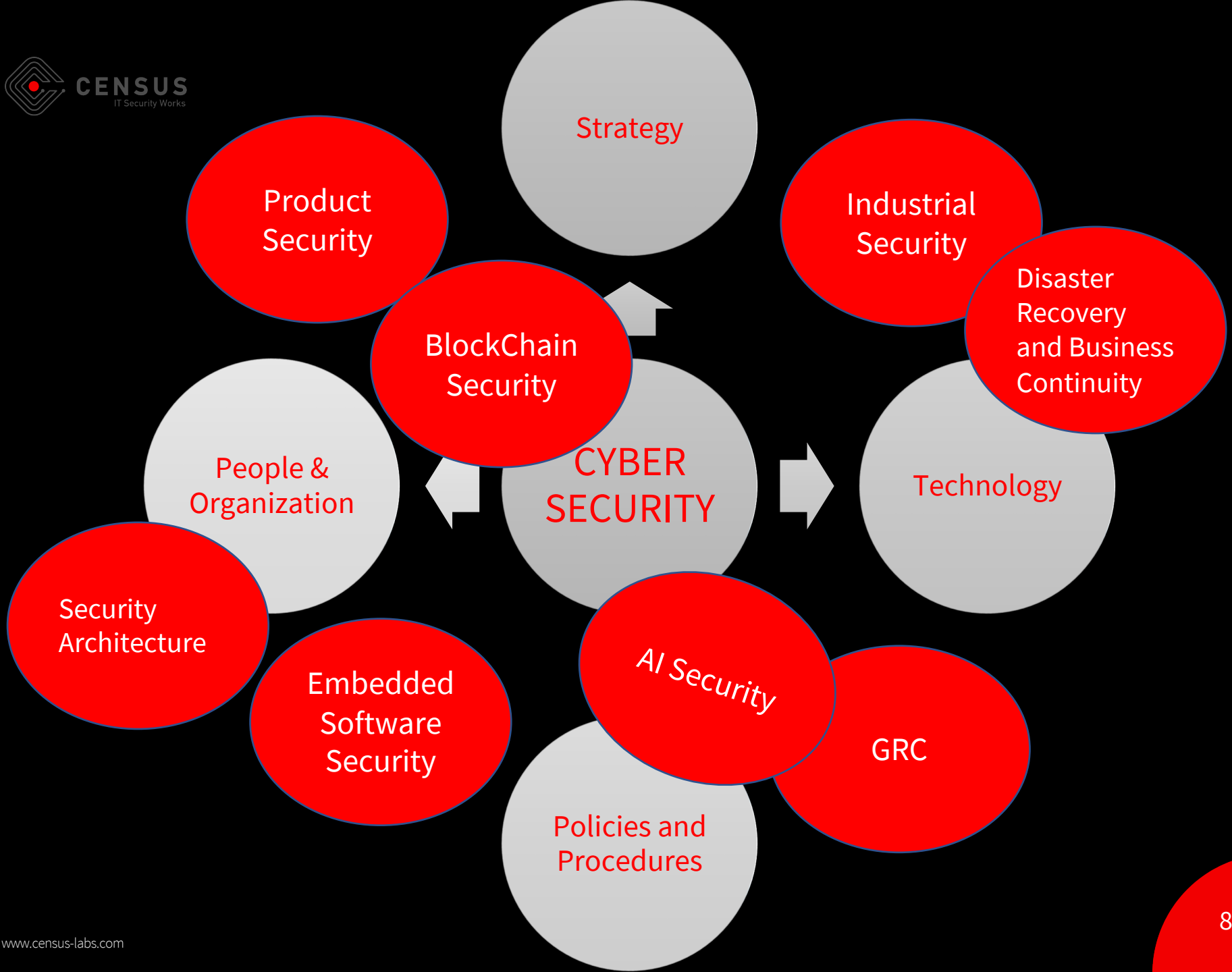

Strategy
Product Security
Industrial Security
People & Organization
CYBER SECURITY
Technology
Embedded Software Security
Policies and Procedures

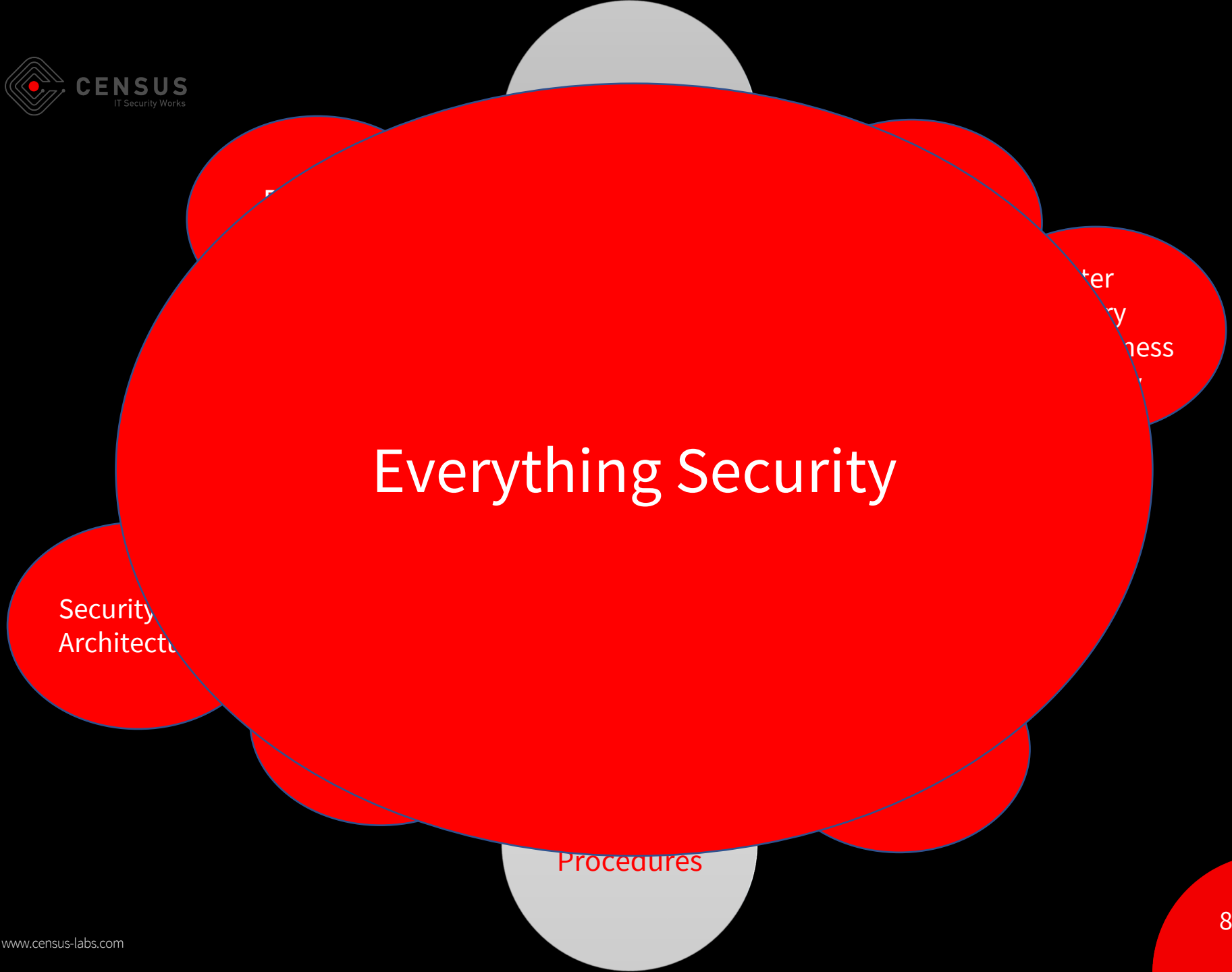

Strategy
Product Security
Industrial Security
People & Organization
CYBER SECURITY
Technology
Embedded Software Security
GRC
Policies and Procedures

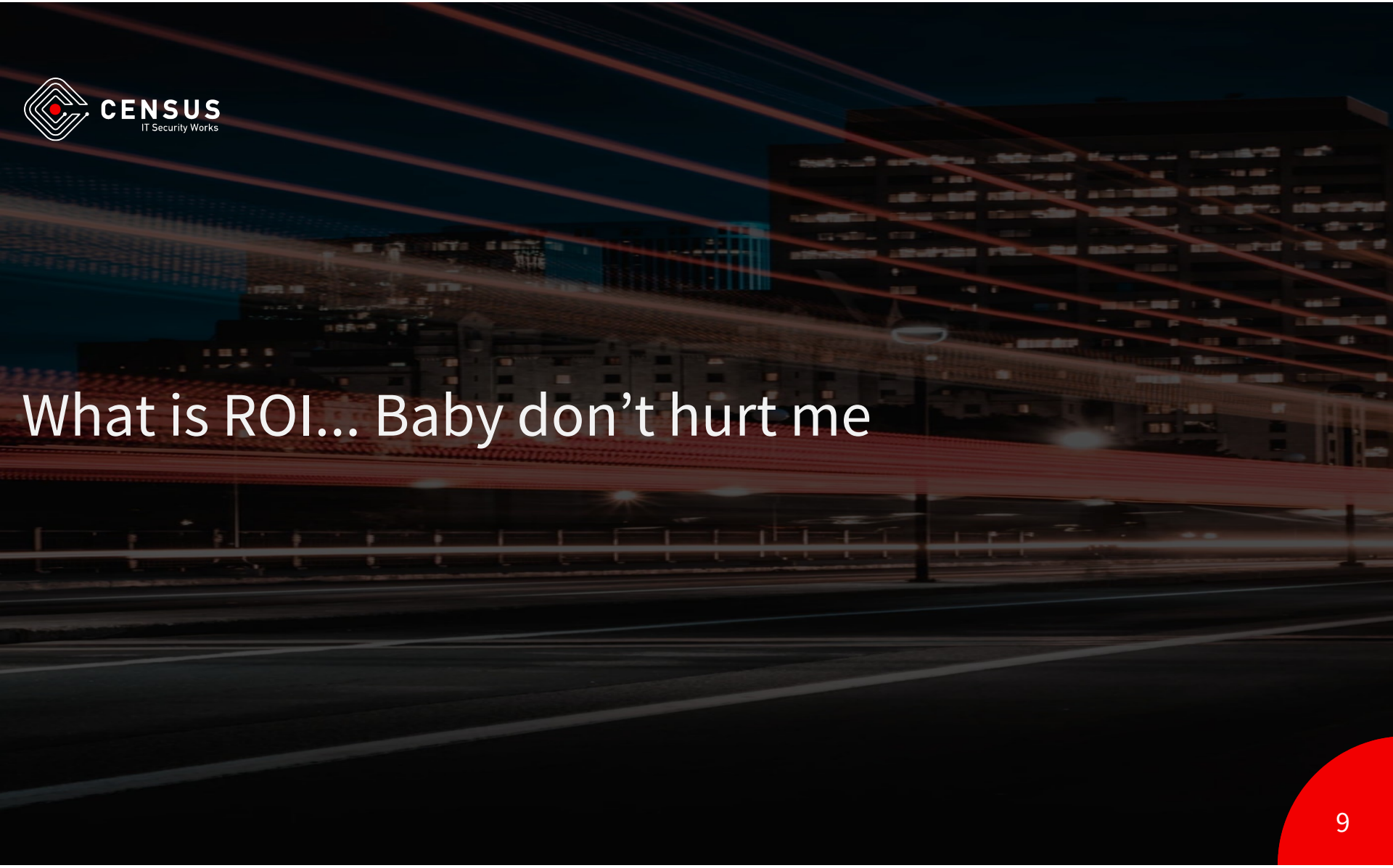

CENSUS
IT Security Works
Strategy
Product Security
Industrial Security
Disaster Recovery and Business Continuity
People & Organization
CYBER SECURITY
Technology
Embedded Software Security
Policies and Procedures
GRC


CENSUS
IT Security Works
Strategy
Product Security
Industrial Security
Disaster Recovery and Business Continuity
People & Organization
CYBER SECURITY
Technology
Security Architecture
Embedded Software Security
GRC
Policies and Procedures


CENSUS
IT Security Works
Strategy
Product Security
Industrial Security
BlockChain Security
Disaster Recovery and Business Continuity
People & Organization
CYBER SECURITY
Technology
Security Architecture
Embedded Software Security
GRC
Policies and Procedures


CENSUS
IT Security Works
Strategy
Product Security
Industrial Security
Disaster Recovery and Business Continuity
BlockChain Security
People & Organization
CYBER SECURITY
Technology
Security Architecture
Embedded Software Security
AI Security
GRC
Policies and Procedures


Everything Security
Procedures


CENSUS
IT Security Works
What is ROI... Baby don’t hurt me

CENSUS
IT Security Works

Return of Investment

- Return on investment (ROI) is the key measure of the **profit** derived from any investment. It is a ratio that compares the **gain or loss** from an investment relative to its cost.

ROI Example

Assume an investor bought 1,000 shares of the hypothetical company Worldwide Wickets Co. at $10 per share. One year later, the investor sold the shares for $12.50. The investor earned dividends of $500 over the one-year holding period. The investor spent a total of $125 on trading commissions in order to buy and sell the shares.

The ROI for this investor can be calculated as follows:

$$\begin{aligned} \text{ROI} &= \frac{(\$12.50 - \$10) \times 1000 + \$500 - \$125}{\$10 \times 1000} \times 100 \\ &= 28.75\% \end{aligned}$$

CENSUS
IT Security Works

What about ROI in Cyber Security

- Return on investment (ROI) in Cyber Security is NOT about the **profit**
- The below approach is based on a specific method where an organisation has defined its Thread Model and already evaluated the cost / loss of every possible event.

Assume in the event of a specific threat (eg Distributed Denial of Service Attack) taking place, the Company will lose 10M.
The investment for one mitigation action (eg a DDoS protection solution) will cost 50K.
The reduced risk will be for example 1M.
The Risk Reduction will be 9M and the investment 50K.

CENSUS
IT Security Works

What about ROI in Cyber Security

- The previous approach covers some portion of the investments on Cyber Security
- But does this approach applies to all the cyber attack cases?

Assume in the event of a specific threat (eg the cargo and loading management application gets hacked) taking place, the Company will lose ???.
The investment for a mitigation action (eg Annual S-SDLC processes for the development, Vendor assessments etc) will cost 200K.
The reduced risk will be ???.

The Risk Reduction will be ??? and the investment 200K.

How can you define the exact cost?
Can you calculate the impact on the reputation?
Can you calculate the time required for the mitigation actions to take place?
Can you be sure about your insurance backpay?
Are there any suppliers' contractual fees?

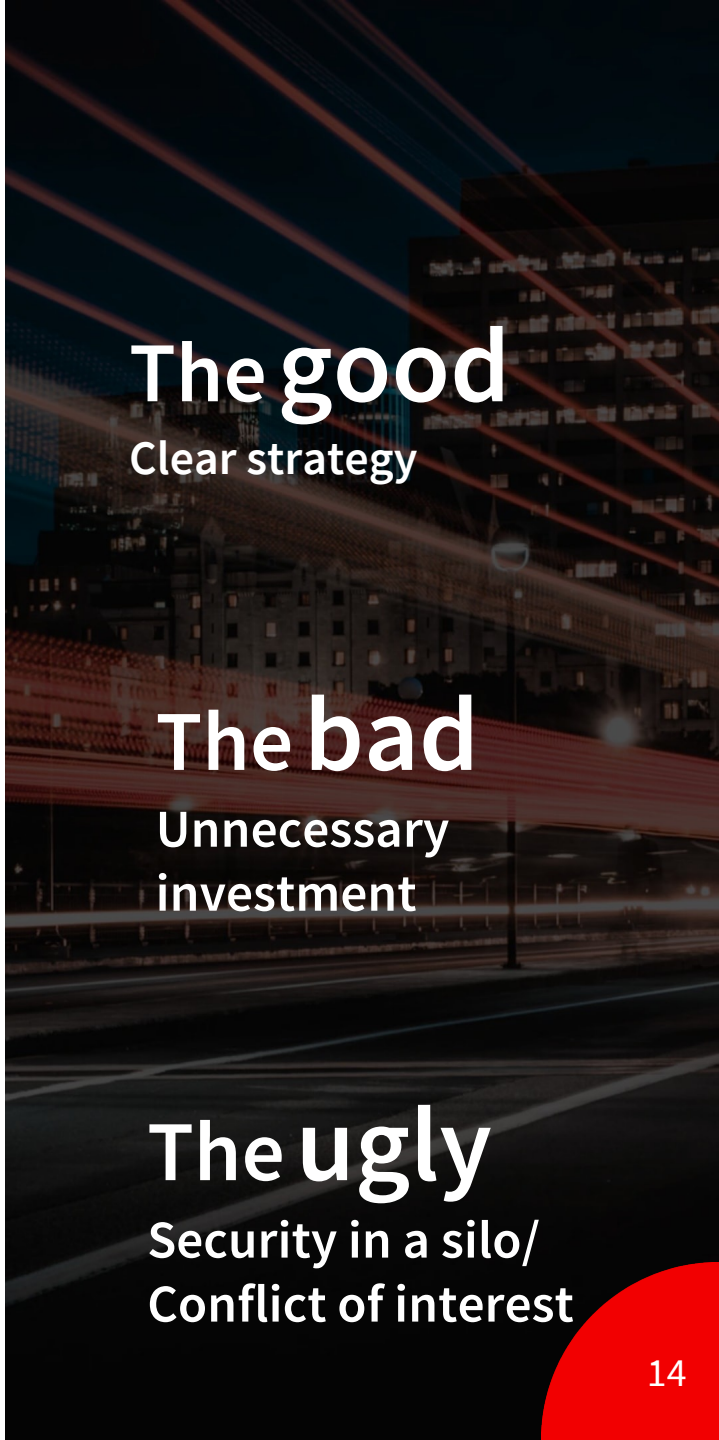
Some good, bad and ugly security investments

CENSUS
IT Security Works

Create a Cyber Security Awareness training strategy
Calculate the current level of your employees security awareness
Calculate the current people related incidents
Implement the awareness training
Run a test to the participants after the training
Implement a more targeted follow up training
Follow the number of incidents in the upcoming months
Communicate the above metrics internally and in the BoD

Company has implemented cyber security measures for the perimeter of the network while the internal network is not segmented at this point.
A new regulatory framework includes the requirement of a security assessment policy and procedures for the company's infrastructure.
The CISO requests approval for external and internal penetration test to be completed in the next 4-6 months.

The CISO / CSO includes in the annual budget the cost patching a specific set of company's servers.
At the same time, the CIO or the CTO has added the cost of purchasing new servers to replace the same set of servers.



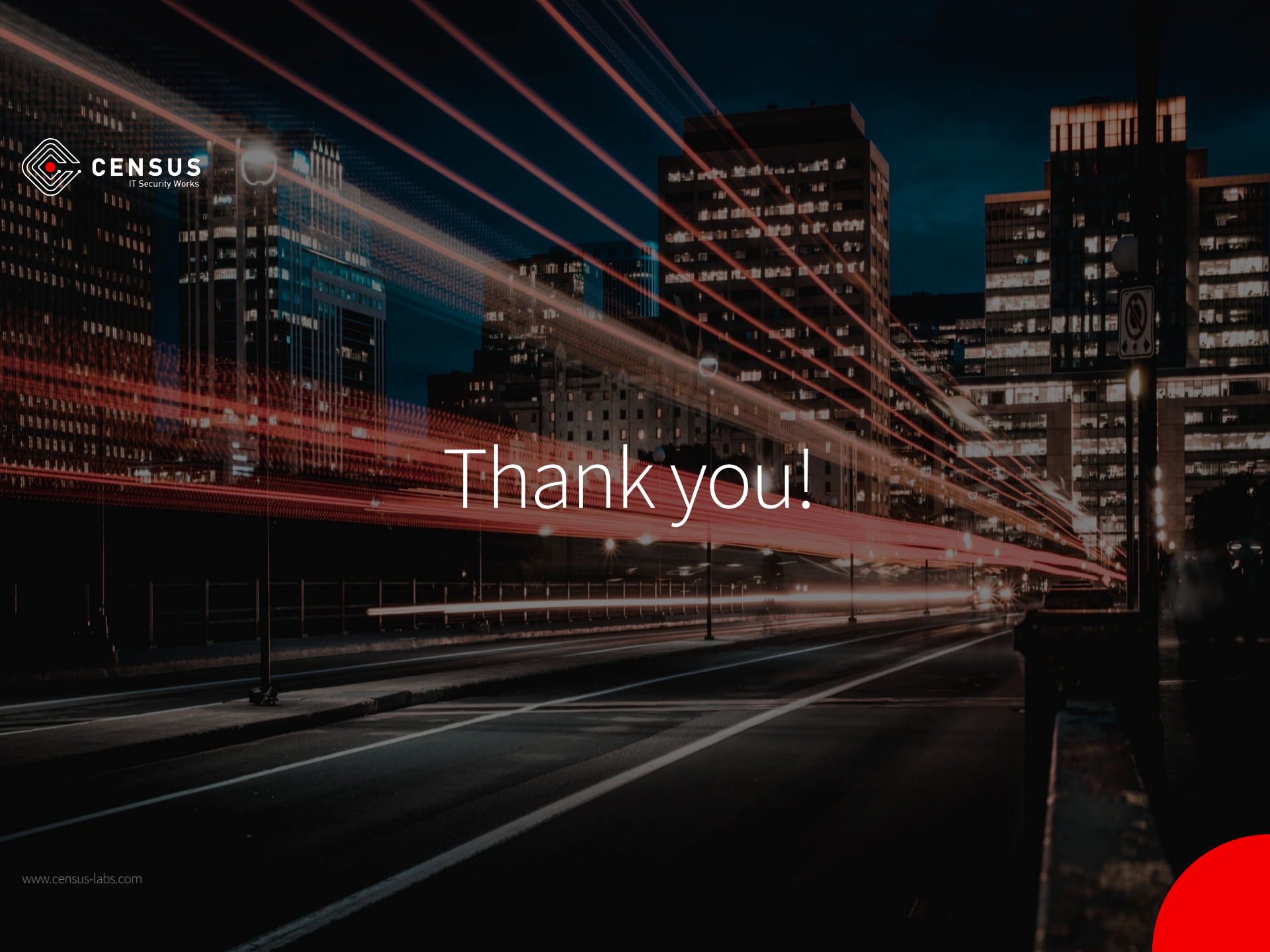

CENSUS
IT Security Works
And now what?

CENSUS
IT Security Works

Cyber Security is a Strategic Investment and not a Cost or Loss

- Start speaking the same language with the BoD
- Use the tools you already have: RISK ASSESSMENT
- Create a clear strategic and update it annually
- Be sure you understand the Risk Appetite of the company
- Use metrics and collect KPIs (eg: Level of Preparedness, Unpatched Systems, Intrusion attempts, Response time data during an event etc)
- CISOs and / or CSOs should be the leadership team


CENSUS
IT Security Works
Questions and possible Answers
You can also find me @CENSUS stand


CENSUS
IT Security Works
Thank you!
www.census-labs.com