ciab FEBRABAN 2016

21 A 23 DE JUNHO
TRANSAMERICA EXPO CENTER
SÃO PAULO - SP

From Cyber Security

to Cyber Defense….

FEBRABAN

Proprietary of Rafael – Advanced Defense Systems Ltd

By Daniel Noy

Senior CERT-IL Program Manager

ISTAR Systems Directorate

RAFAEL
ADVANCED DEFENSE SYSTEMS LTD.

Agenda

- Introduction
- A Glimpse to Cyber History
- The challenges
- Cybernetic meets the physics
- Cyber and Intelligence
- Cyber Defense Landscape in the Financial Sector
- Summary

RAFAEL

ADVANCED DEFENSE SYSTEMS LTD.

Introduction

Who am I?

PERSONAL

Live in Israel,
BS.C and MS.C in Information management systems & Industrial Engineering
Love sports

PROFESSIONAL

Managed several projects in the cyber arena delivering cyber intelligence solutions

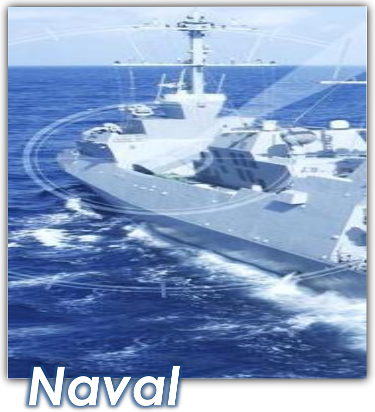
Nowadays performs a role as a Senior Director and Project Manager for National CSIRT

MILITARY

Colonel (Ret.) served in the Intelligence Corps for more than 20 years.
Managed all intelligence acquisitions mission at USA MOD- in New York for IDF

Rafael at a Glance

Land


Naval

Air & Space

Cyber

$2 Billions+
Defense
Company

4 Domains
Cyber , Air,
Land & Sea

+ 7,000
employees in
Israel

+60% of
Engineers &
Academics

The Prime Contractor for Israel’s National CSIRT

ically forging ahead with the development of radar technology on the basis of our many years of experience and

Some of the innovative technology that Airbus Defence and Space has actually turned into current, mar-

cy modules, thus providing the latest radar technology in the area of electronic beam control.

Rafael Has Been Selected to Head Israel’s National CERT Programme

Rafael Advanced Defense Systems Ltd., developer and manufacturer of ground-breaking technologies such as Iron Dome, Trophy and David’s Sling, has been selected by the Israeli government to head Israel’s Computer Emergency Response Team (CERT) programme.

Rafael will serve as the prime contractor of the programme in cooperation with Israeli and global IT corporations – EMC, IBM, Matrix and Cisco. Together these companies will develop solutions designed to provide Israel’s cyber defence programme with advanced security and defence capabilities for detection, monitoring and handling of cyber threats.

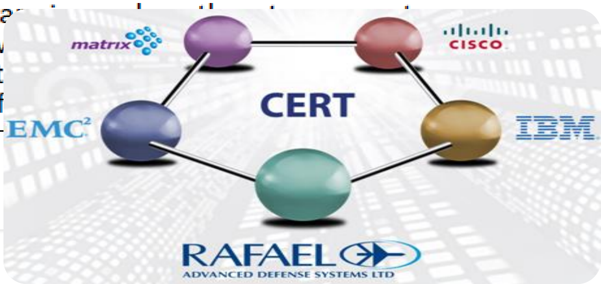
The programme will combine a variety of IT infrastructures and advanced tools to assist civilian companies and government offices in their efforts to prevent and handle cyber attacks.

The team of companies headed by Rafael will combine proven Israeli and international experience and know-how, as well as state-of-the-art solutions and products.

Brigadier General Ariel Karo (retd), head of Rafael’s C4I and Cyber Directorate, stated that the solutions to be provided by Rafael and its partners will comprise a significant contribution to Israel’s effort to bolster its defence against cyber threats. Karo added, ‘Our solution is conceptually unique, and is designed to analyse and suit the proper mode of operation to the most complex threats in the global cyber arena.”

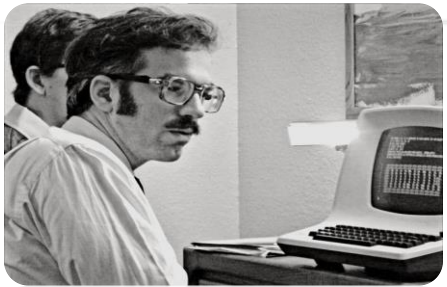
VADM (retd), Yedidia Yaari, CEO and President of Rafael, said, “Rafael’s selection by the Israeli government is a strategic development for the company. Rafael is known for its technological legacy and successes with systems such as Iron Dome, Trophy and David’s Sling. We are now ready to leverage our expertise in cyber technology, together with our new partners, to lead Israel’s battle against the ever-growing and cha of our v suring t State of

66 FORCE | August 2015



A Glimpse to Cyber History

Short history of Cyber Security



VS.

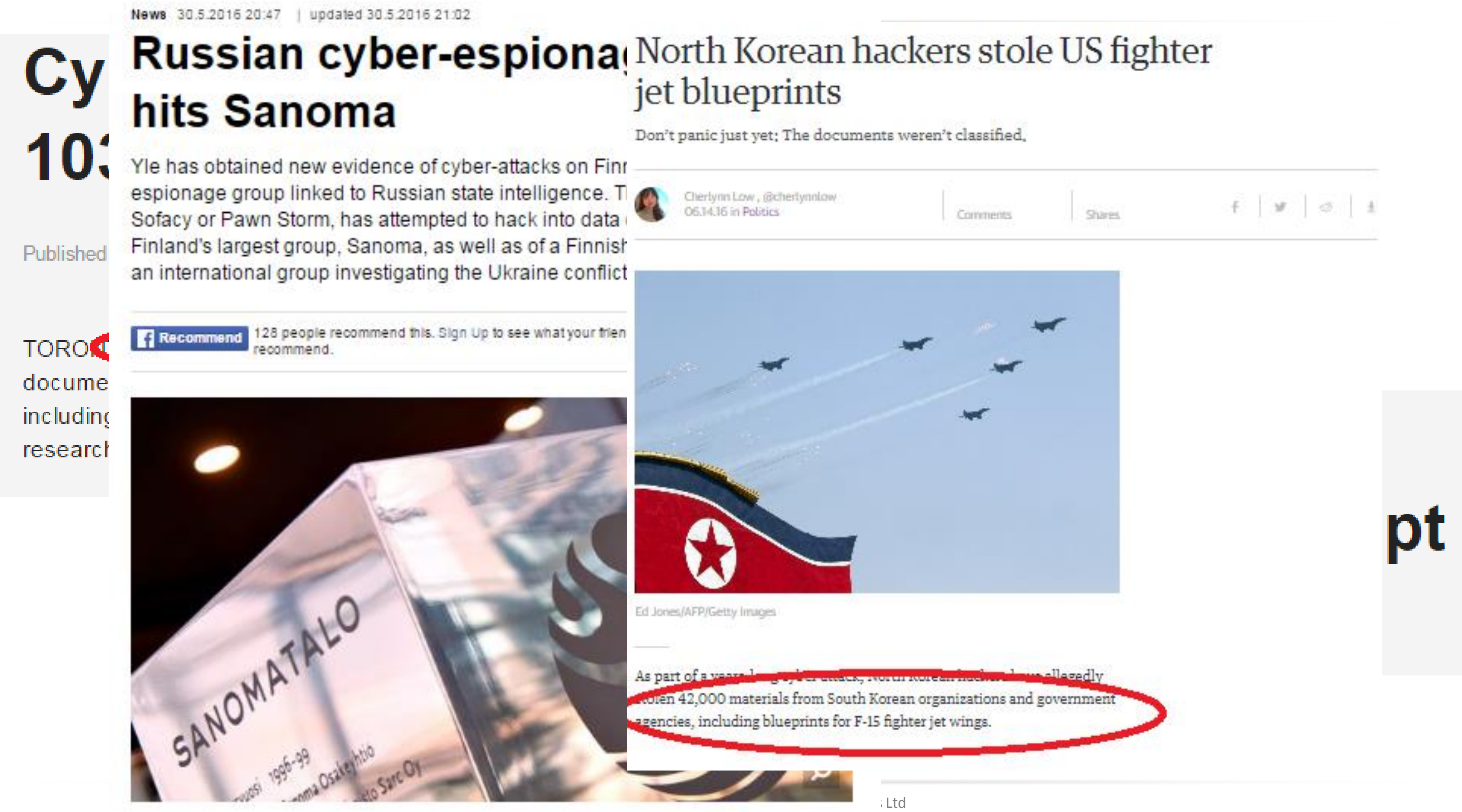
KASPERSKY
ANTI-VIRUS
AVG
McAfee
ca
INTERNET SECURITY SUITE 2010
Microsoft Security Essentials
bitdefender
F-Secure
avast! be free
AVIRA
eset
NOD32 antivirus

Short history of Cyber Security

VS.

pic by: Dor Garbash

Nations against Nations



Cy
103

Published

TORO
docume
including
research

pt

News 30.5.2016 20:47 | updated 30.5.2016 21:02

Russian cyber-espiona hits Sanoma

Yle has obtained new evidence of cyber-attacks on Finn espionage group linked to Russian state intelligence. T Sofacy or Pawn Storm, has attempted to hack into data Finland's largest group, Sanoma, as well as of a Finnish an international group investigating the Ukraine conflict

Recommend 128 people recommend this. Sign Up to see what your frien recommend.

North Korean hackers stole US fighter jet blueprints

Don't panic just yet; The documents weren't classified.

Cherlynn Low , @cherlynnlow
06.14.16 in Politics

Comments

Shares

Ed Jones/AFP/Getty Images

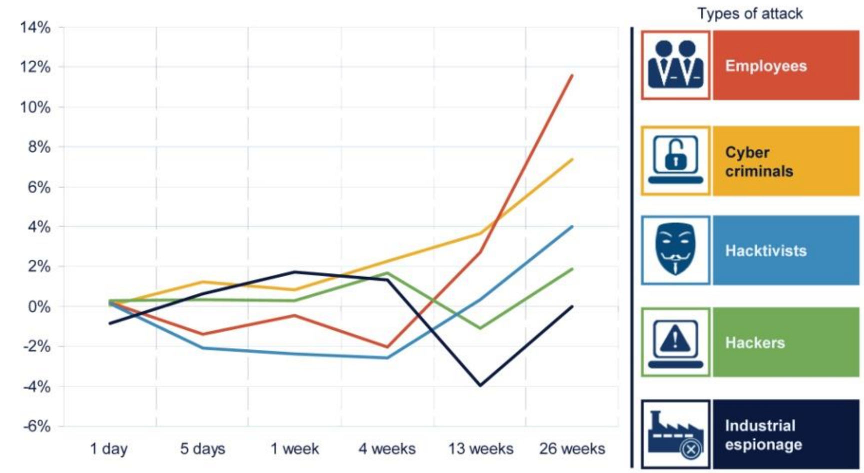
As part of a years-long cyber attack, North Korean hackers have allegedly stolen 42,000 materials from South Korean organizations and government agencies, including blueprints for F-15 fighter jet wings.

Ltd

Situation

Malware continues to **change at a rapid pace**, as evidenced by **new types of high-tech, military-grade malicious code** grabbing headlines such as Stuxnet, Duqu and Flame.

Which type of cyber attack spooks the markets most?



Freshfields Bruckhaus Deringer

Cyber Domain as a Battlefield

The cyber domain is becoming to be a **battlefield**; therefore you need a **military standard** solution even for the private sector and especially in the the **financial arena**.

Cyber Domain as a Battlefield

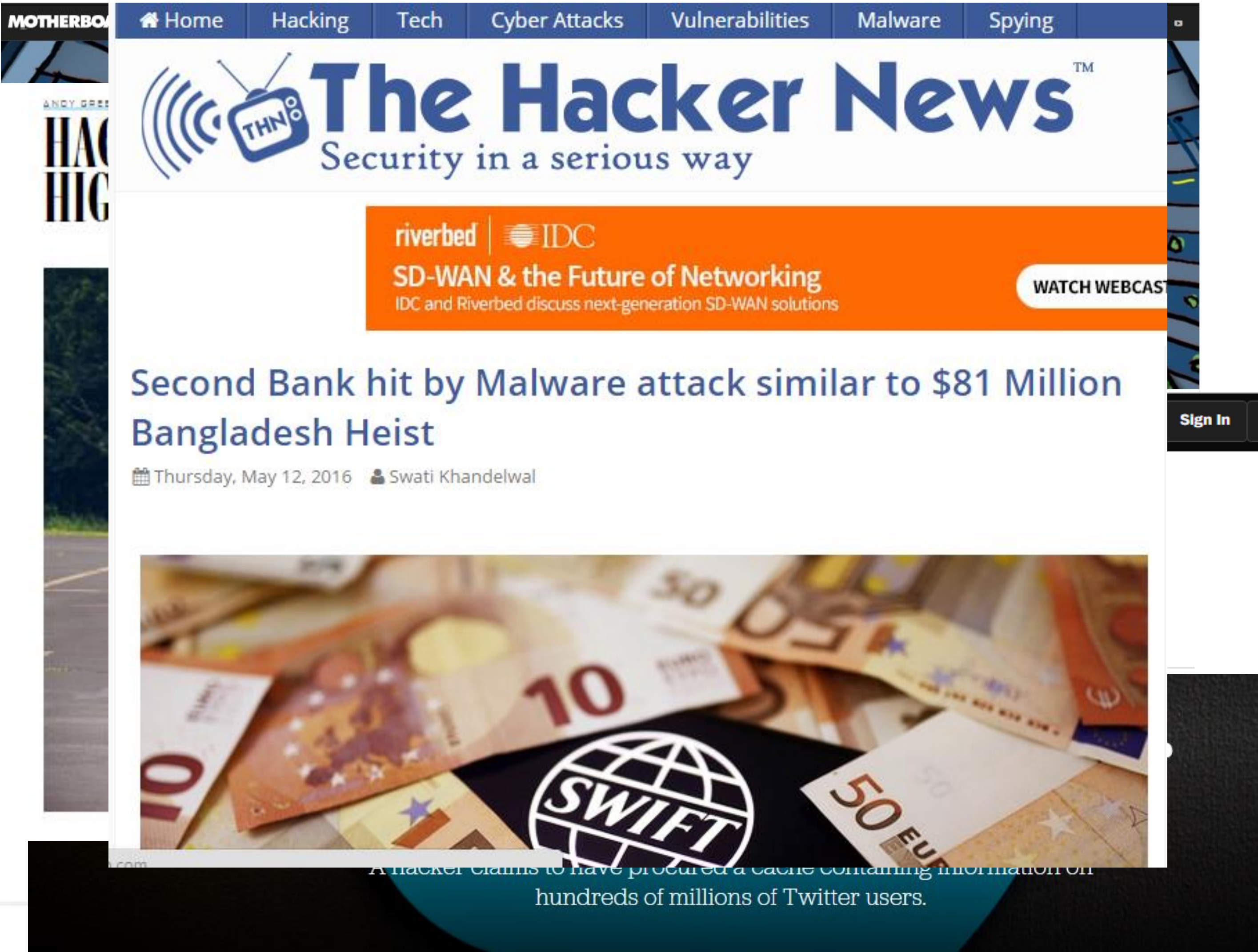
The best way to achieve this goal is to **merge** between the **know how & Intelligence gathered** from the defense with a company that has a lot of **experience in financial domain**.

The challenges

The motivation progress

Attack Damages

- Financial
- Reputation
- Privacy
- Physical
- And more



The Hacker News™
Security in a serious way

riverbed | IDC
SD-WAN & the Future of Networking
IDC and Riverbed discuss next-generation SD-WAN solutions
WATCH WEBCAST

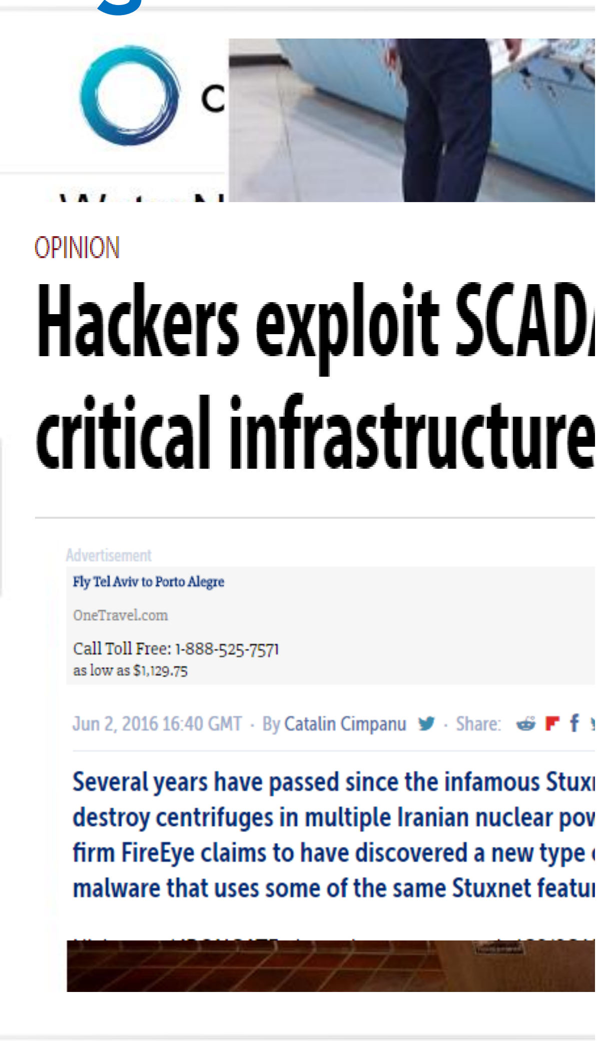
Second Bank hit by Malware attack similar to $81 Million Bangladesh Heist

Thursday, May 12, 2016 Swati Khandelwal

A hacker claims to have procured a cache containing information on hundreds of millions of Twitter users.

Attack Damages

- Financial
- Reputation
- Privacy
- Physical
- And more



OPINION

Hackers exploit SCAD
critical infrastructure

Advertisement

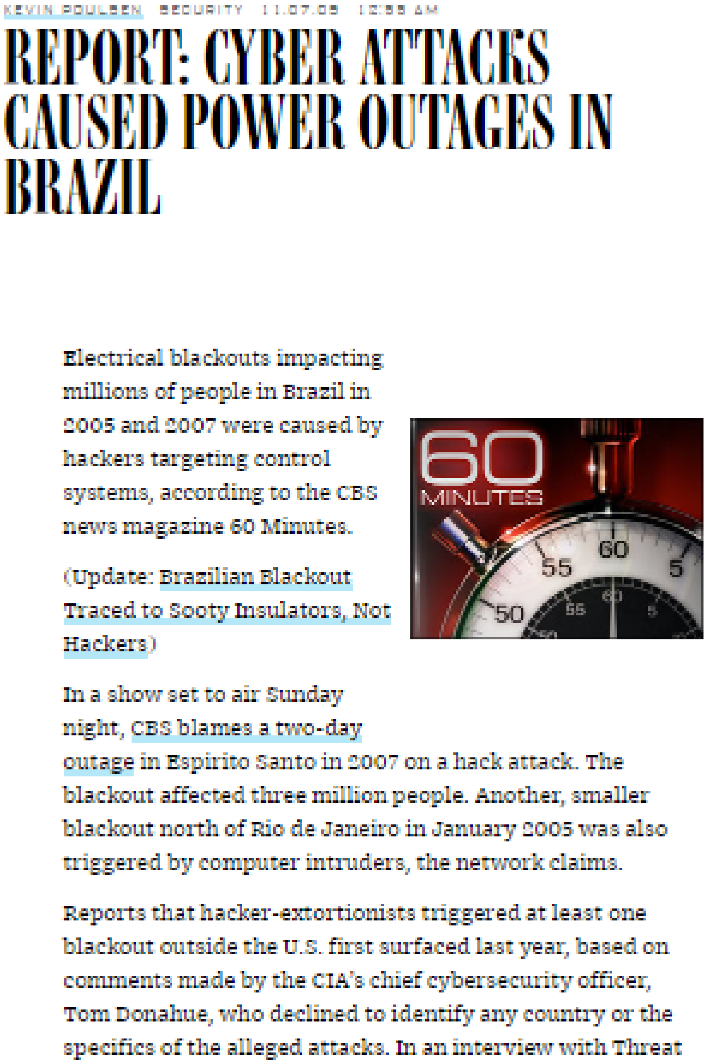
Fly Tel Aviv to Porto Alegre

OneTravel.com

Call Toll Free: 1-888-525-7571
as low as $1,129.75

Jun 2, 2016 16:40 GMT · By Catalin Cimpanu · Share:

Several years have passed since the infamous Stuxı destroy centrifuges in multiple Iranian nuclear pov firm FireEye claims to have discovered a new type (malware that uses some of the same Stuxnet featuı



KEVIN POULSEN SECURITY 11.07.09 12:55 AM

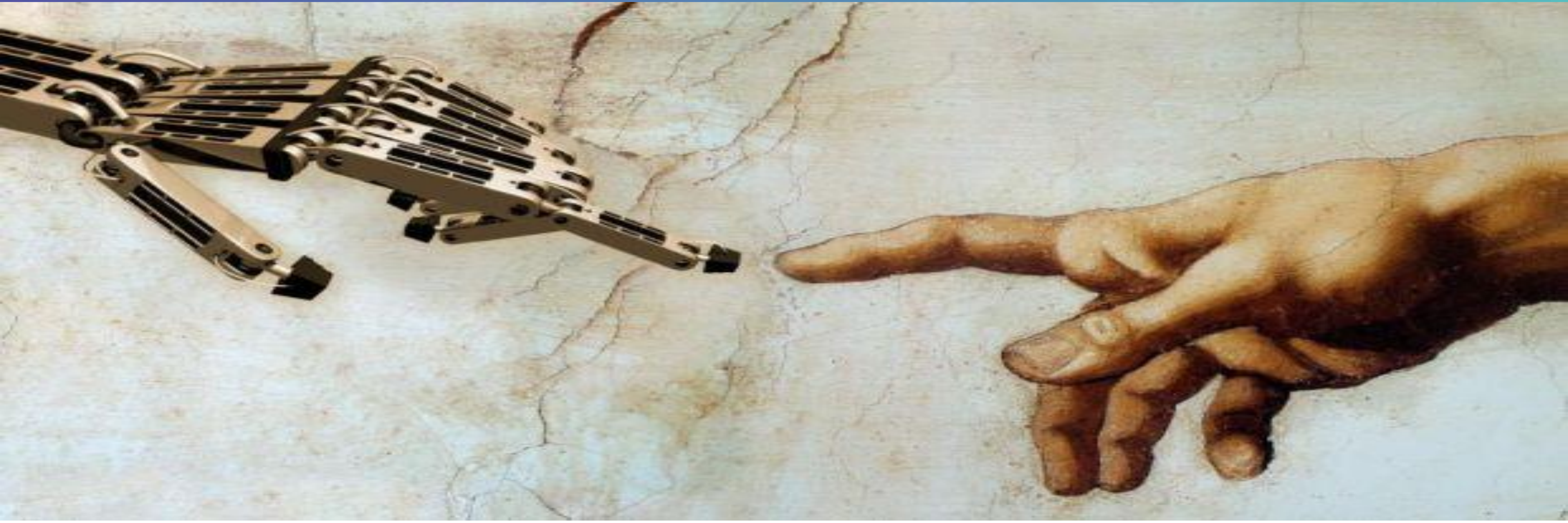
REPORT: CYBER ATTACKS CAUSED POWER OUTAGES IN BRAZIL

Electrical blackouts impacting millions of people in Brazil in 2005 and 2007 were caused by hackers targeting control systems, according to the CBS news magazine 60 Minutes.

(Update: Brazilian Blackout Traced to Sooty Insulators, Not Hackers)

In a show set to air Sunday night, CBS blames a two-day outage in Espirito Santo in 2007 on a hack attack. The blackout affected three million people. Another, smaller blackout north of Rio de Janeiro in January 2005 was also triggered by computer intruders, the network claims.

Reports that hacker-extortionists triggered at least one blackout outside the U.S. first surfaced last year, based on comments made by the CIA's chief cybersecurity officer, Tom Donahue, who declined to identify any country or the specifics of the alleged attacks. In an interview with Threat



Cybernetic meets the Physical

The physical world

Public Order

Traffic lights,
communication

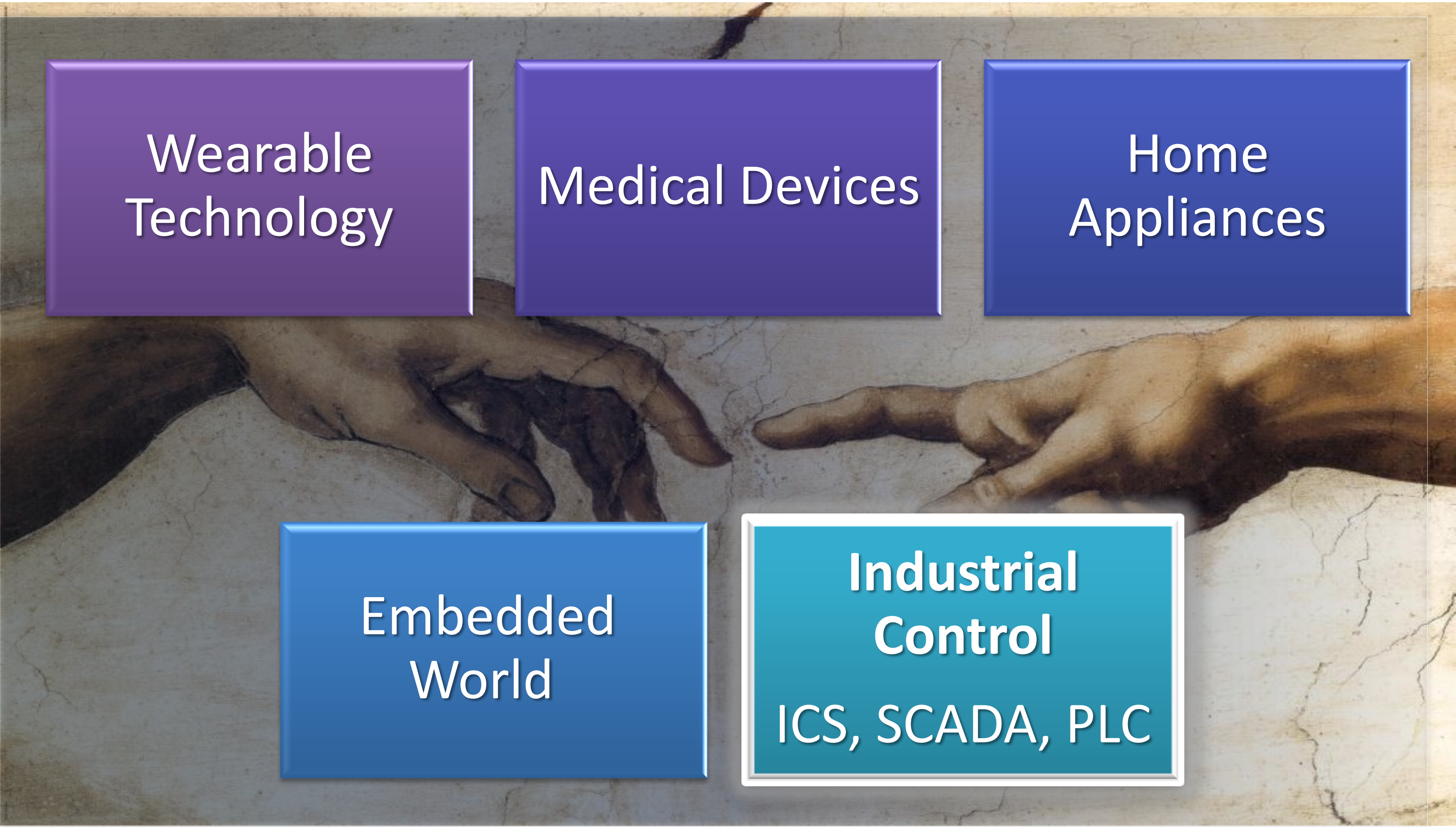
Critical infrastructure

Electricity,
water, gas.

Our life

Car, insulin pump,
elevator,
microwave

The cybernetic meets the physical



Wearable Technology

Medical Devices

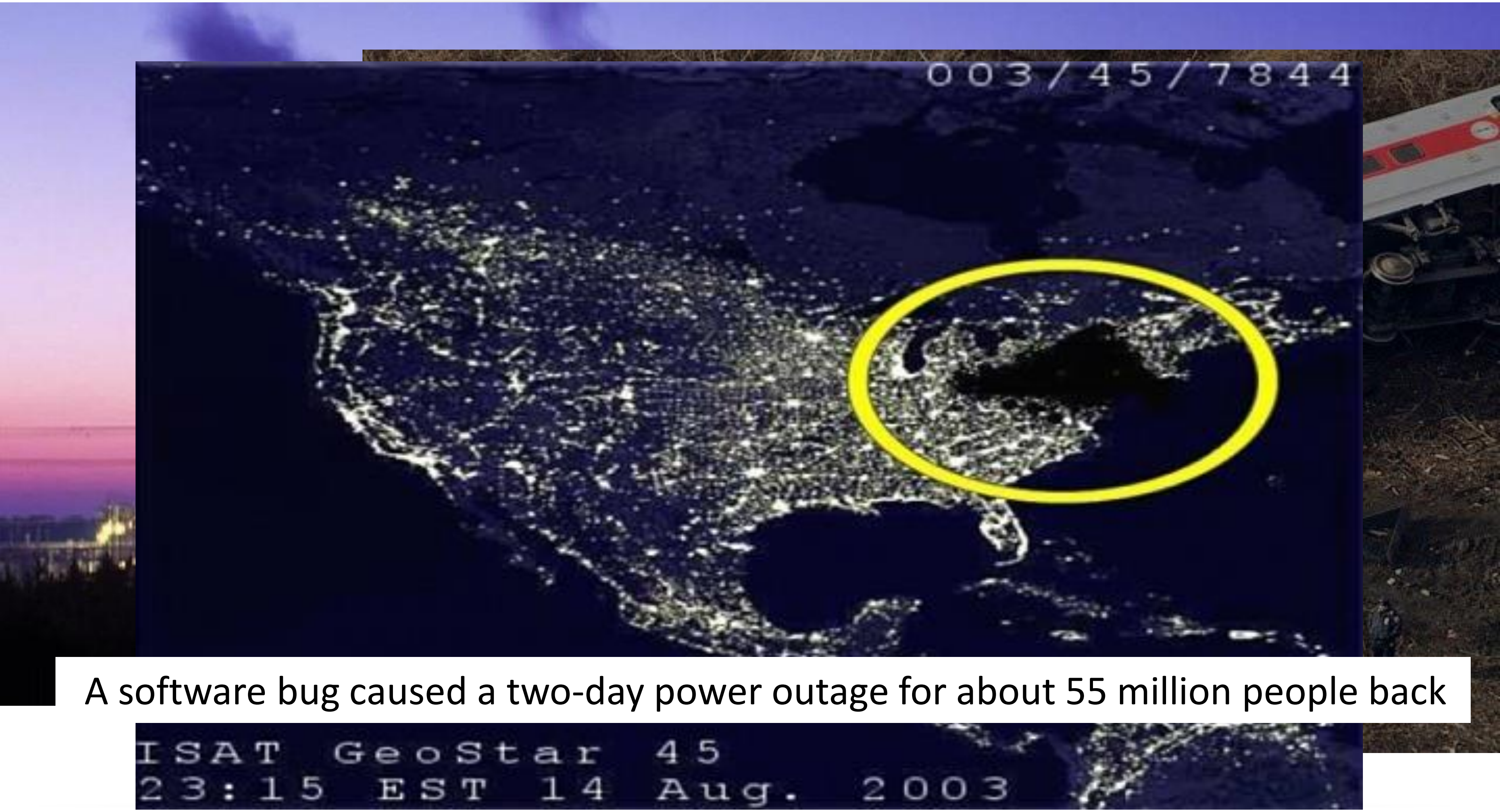
Home Appliances

Embedded World

Industrial Control

ICS, SCADA, PLC

What might be the damages???

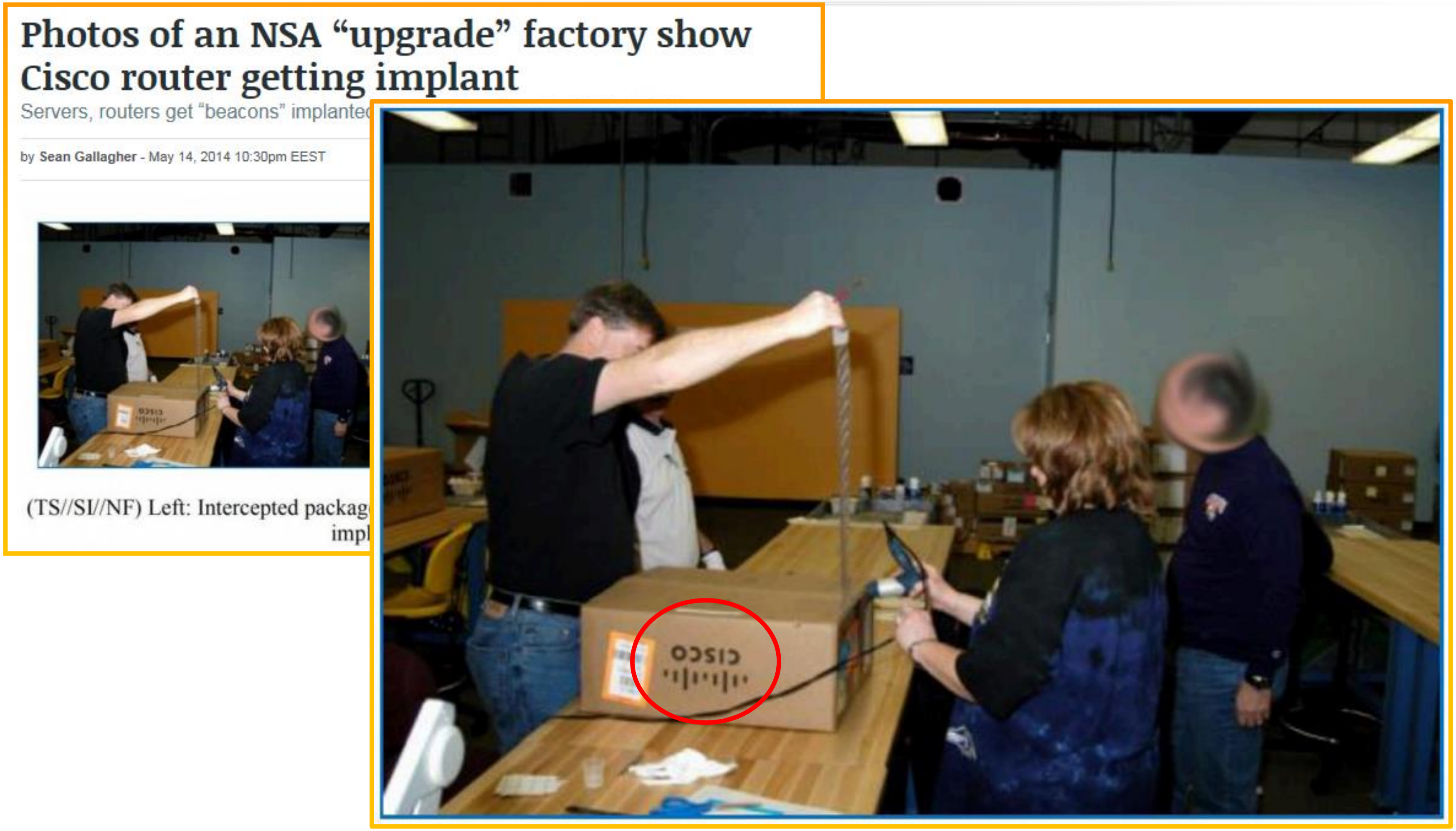


A software bug caused a two-day power outage for about 55 million people back

So , What is a the meaning of Cyber Defense ?

- Know your Enemy
- Adopt Intelligence as part of the holistic solution
- Need to be one step a head
- Be Proactive and learn from Reactive
- Do not use only existing security tools
- Orchestrated architecture

Attack Scenario - “New” Tampered Equipment



Photos of an NSA “upgrade” factory show Cisco router getting implant

Servers, routers get “beacons” implante

by Sean Gallagher - May 14, 2014 10:30pm EEST

(TS//SI//NF) Left: Intercepted packag
impl

If you think that you are <u>protected</u> in the **IT**

Start to Think Differently

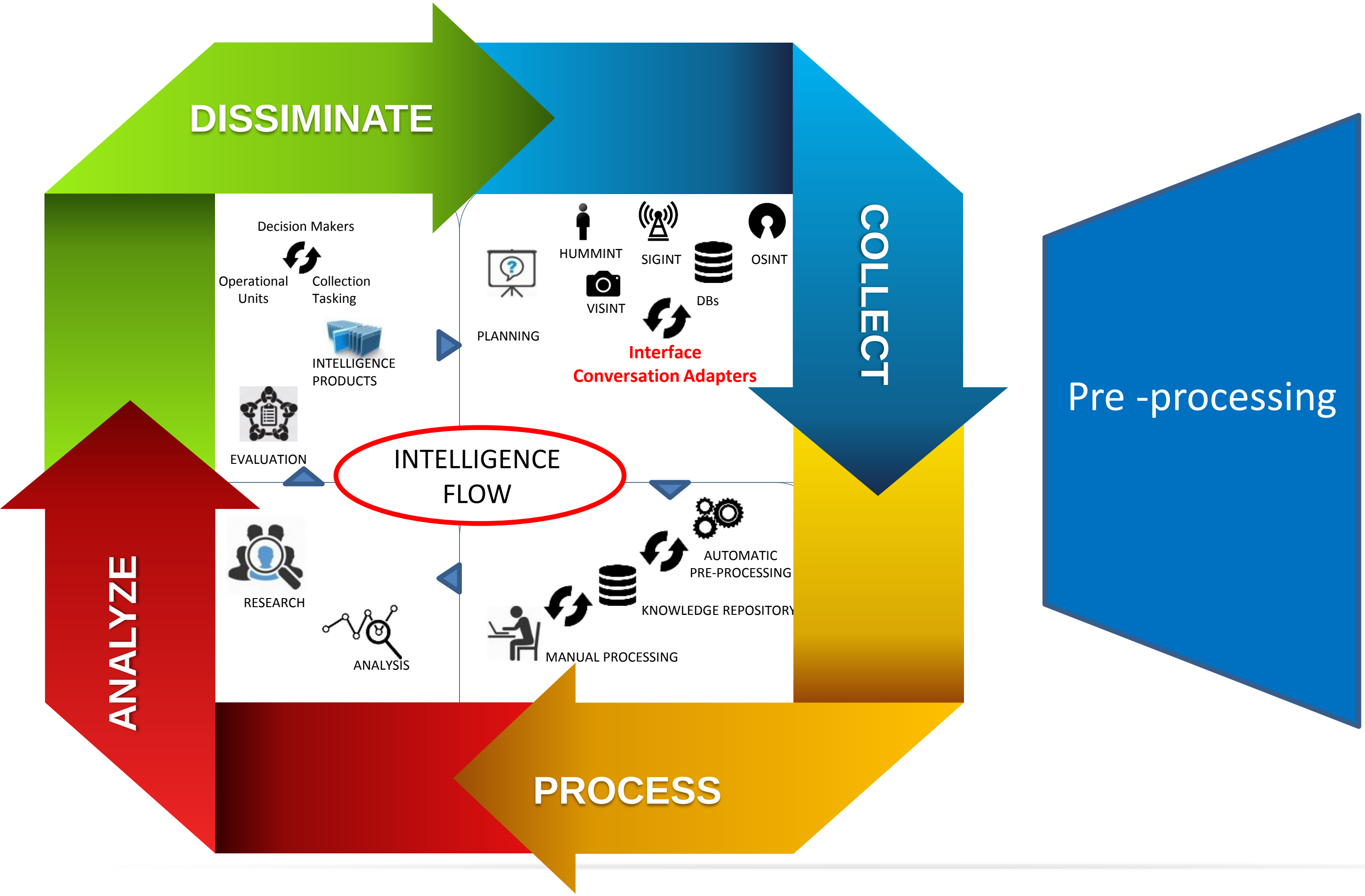
- And more

Cyber & Intelligence

Traditional Intelligence disciplines

….but , what about Cyber ?

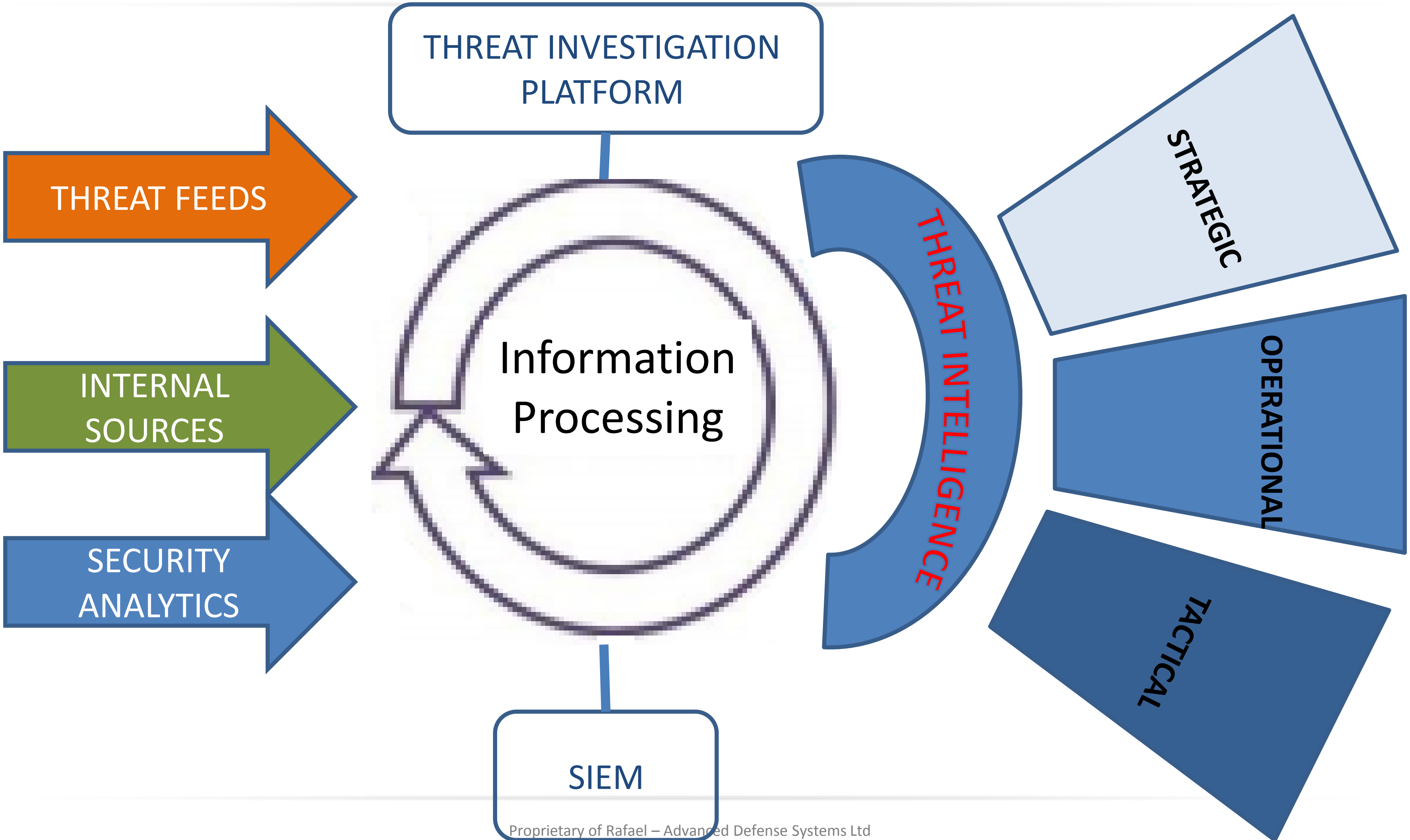
Sensors

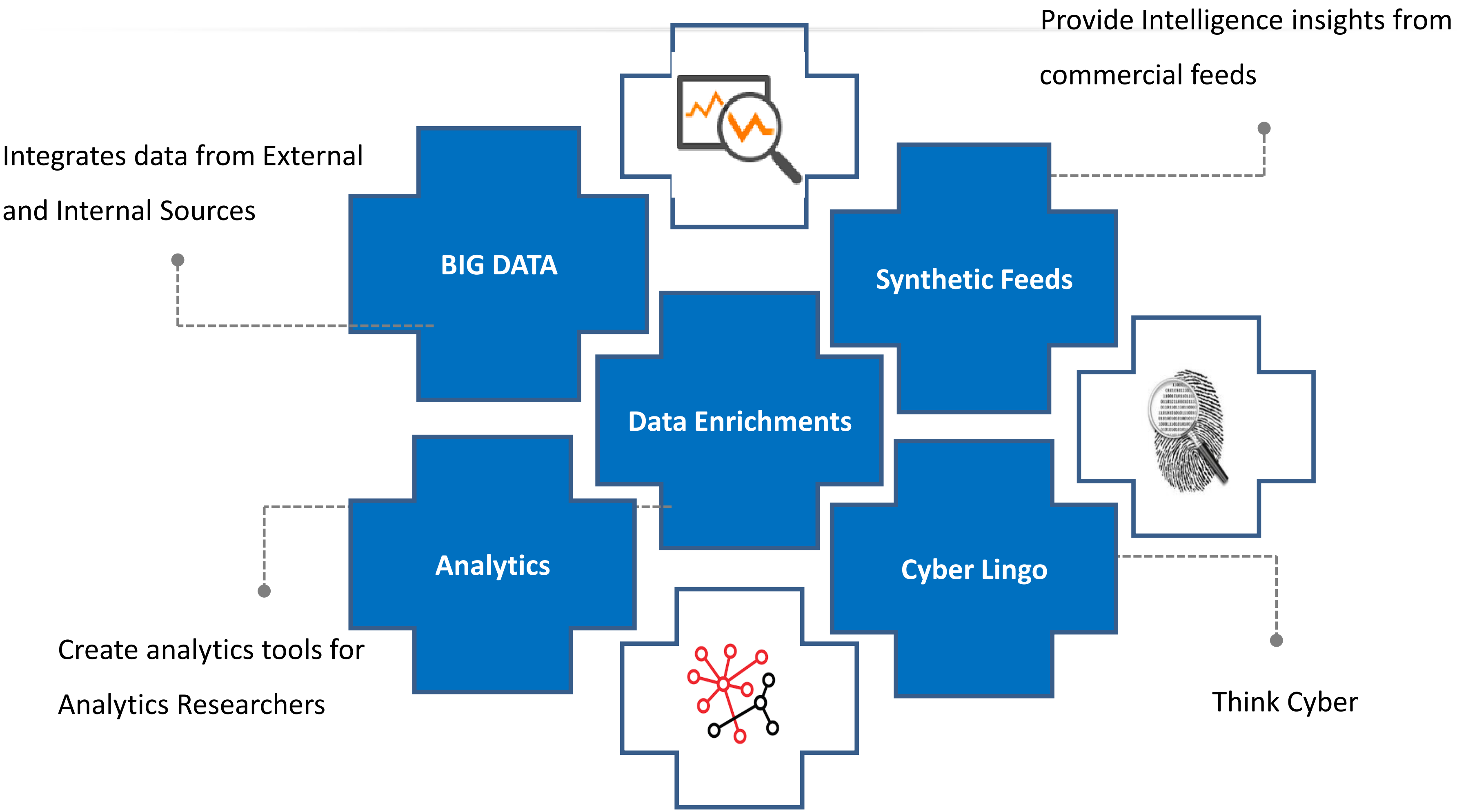


SIGINT
OSINT
VISINT
HUMINT
CYBER

Collection

Cyber Threat Intelligence





Provide Intelligence insights from commercial feeds

Integrates data from External and Internal Sources

Create analytics tools for Analytics Researchers

Think Cyber

Intelligence Threat Platform - Using Common Ling

- Using STIX firmat as a common language to describe Cyber Events (A very rich lingo)
- Combination of the operational experience and best analytics tools
- The best platform and lingo to share Cyber info with partners and customers

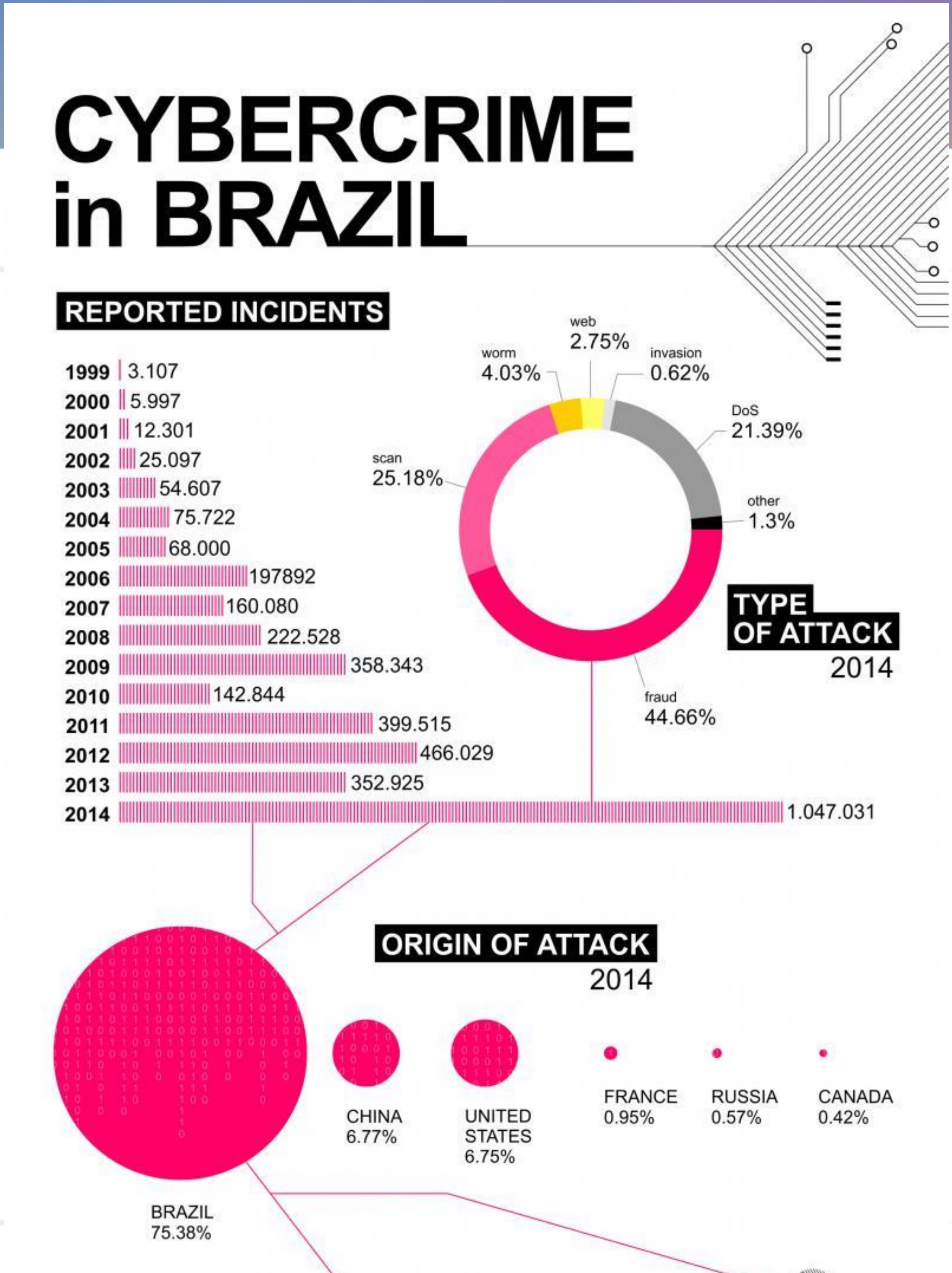
Cyber Defense Landscape in the Financial Sector

Cyber Defense Landscape in the Financial Sector

Banks in Brazil

- 60% of the country's 200 million citizens are connected to the Internet.
- At least 45% of all banking transactions in Brazil are **digital**
- Brazil, with **130 machines per 100,000 adults**, has a **greater density of ATMs**
    - UK (127), France (109), or Germany (116)
- Banks and financial institutions considered part of the national critical infrastructure

Situation in Brazil



Business Orientation Changes

E-banking vs. Banking

Migration to cloud services

ATM Malwares

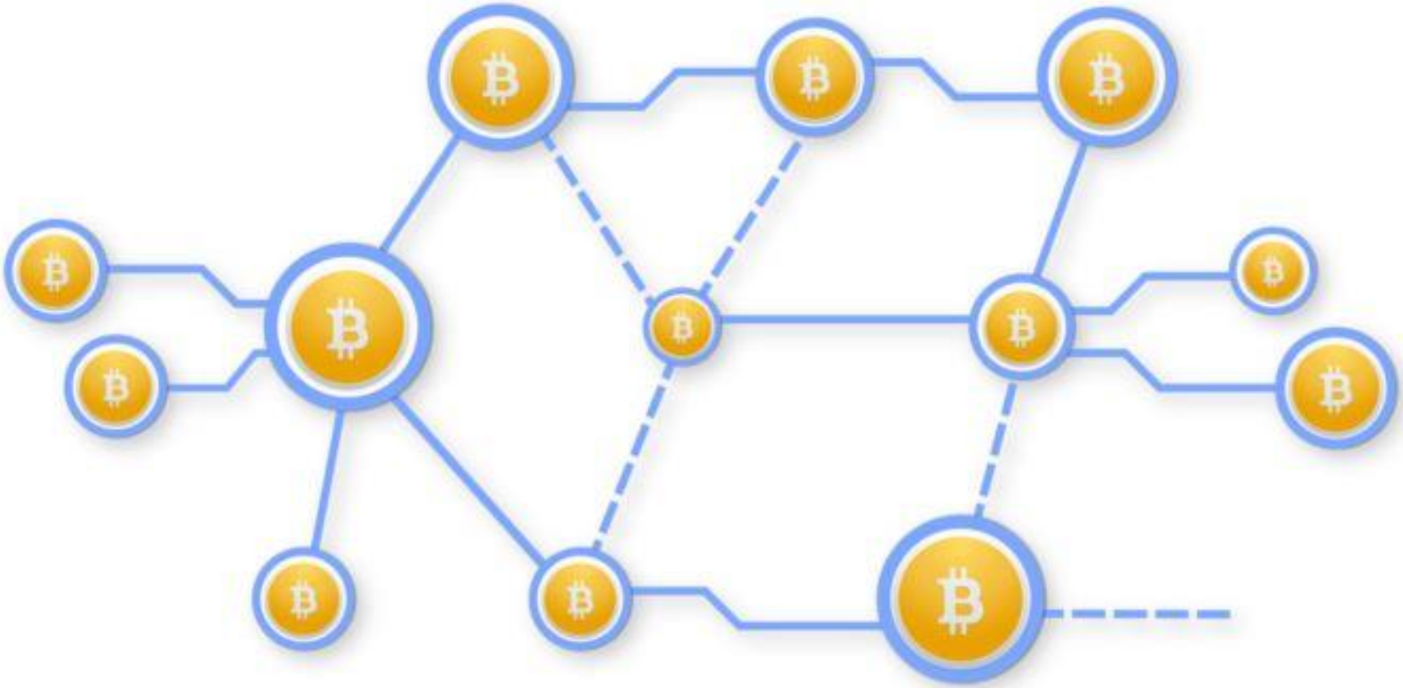
Weak cybercrime laws and regulations

Financial losses from cybercrime

- More Cyber Threats on Banks

Bitcoin Network -

A slow transactions due to a spam attack



www.newsbtc.com

Cloud Services - security threats

- Cloud providers typically deploy security controls to protect their environments
- organizations are responsible for protecting their own data in the cloud.
- organizations must use multifactor authentication and encryption to protect against data breaches

Cloud Services - security threats

Compromised credentials and broken authentication

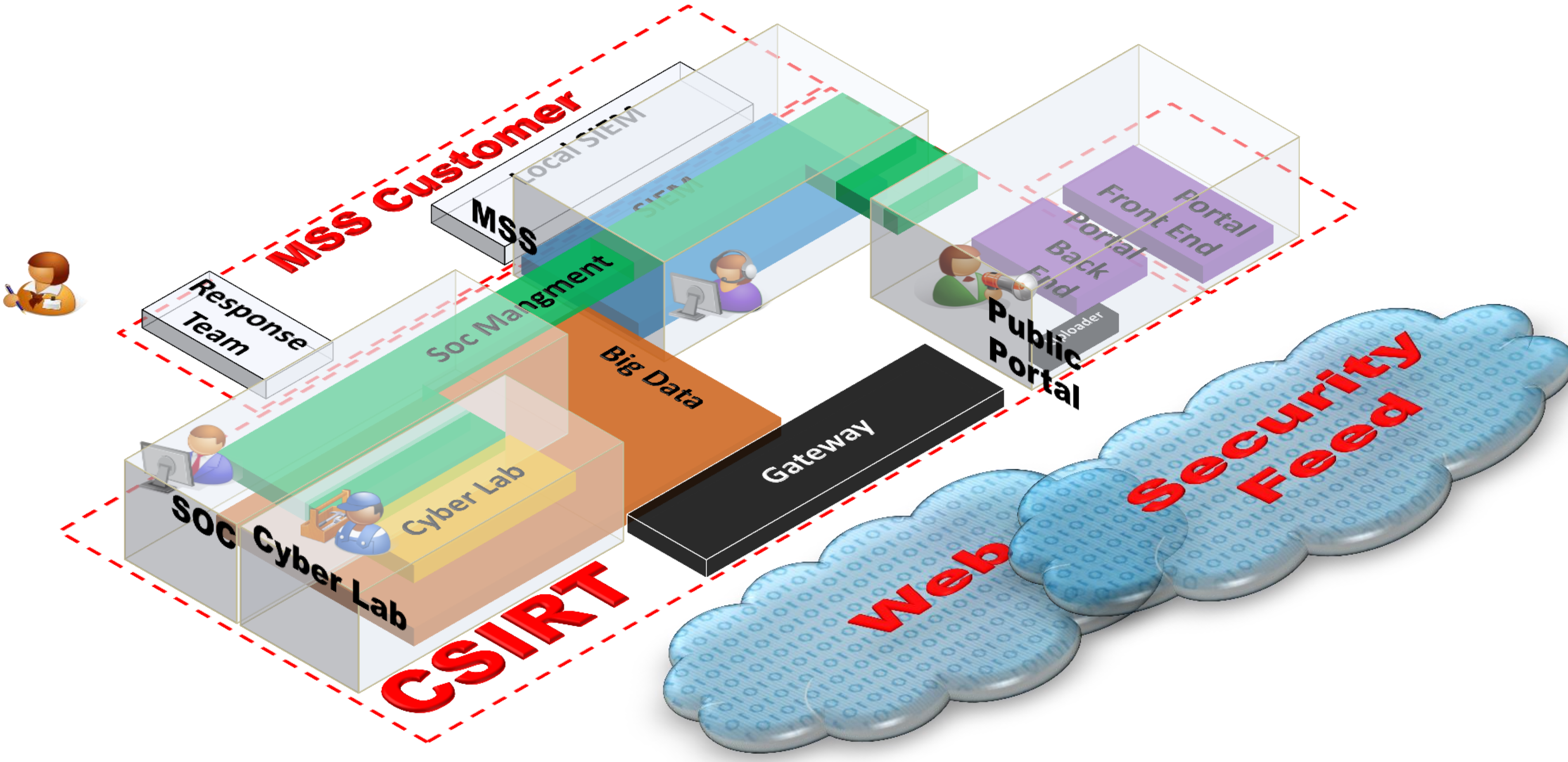
- The Anthem breach, which exposed more than 80 million customer records, was the result of stolen user credentials

Cloud Services - security threats

- Hacked interfaces and APIs
- Exploited system vulnerabilities
- Account hijacking
- Malicious insiders
- The APT parasite
- Inadequate diligence
- DDoS attacks
- Shared technology, shared dangers

CSIRT Solution - Architecture and Key points

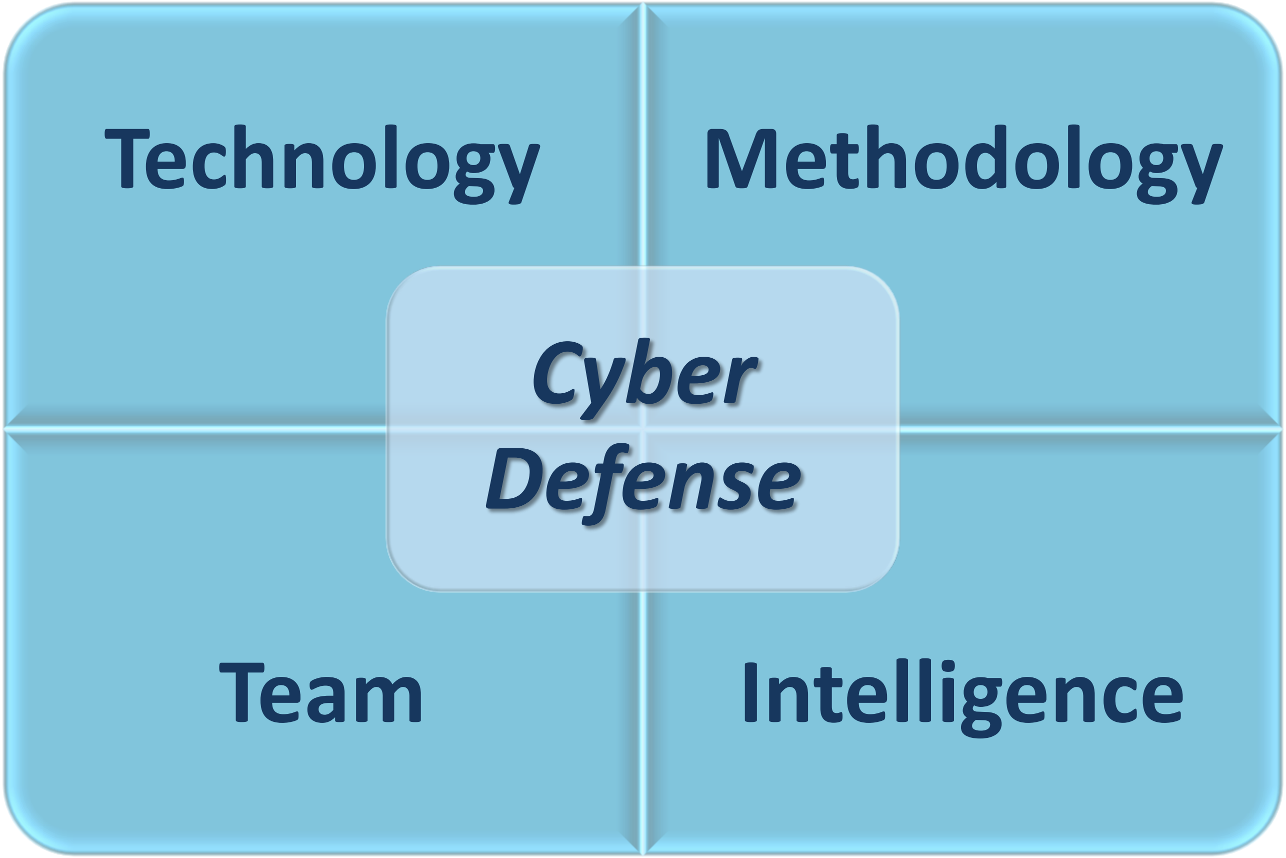
CSIRT Architecture



Defense by Design

- CSIRT is a **very** **attractive** target
- Design **Methodology**
  - Multi layer
  - Overlapping
  - Extra attention to the Cyber lab and internet
  - Threat Intelligence Platform
- **Integrate** different existing security's platforms
- Cybernetic vs. Physical

How to defend your organization



Technology

Methodology

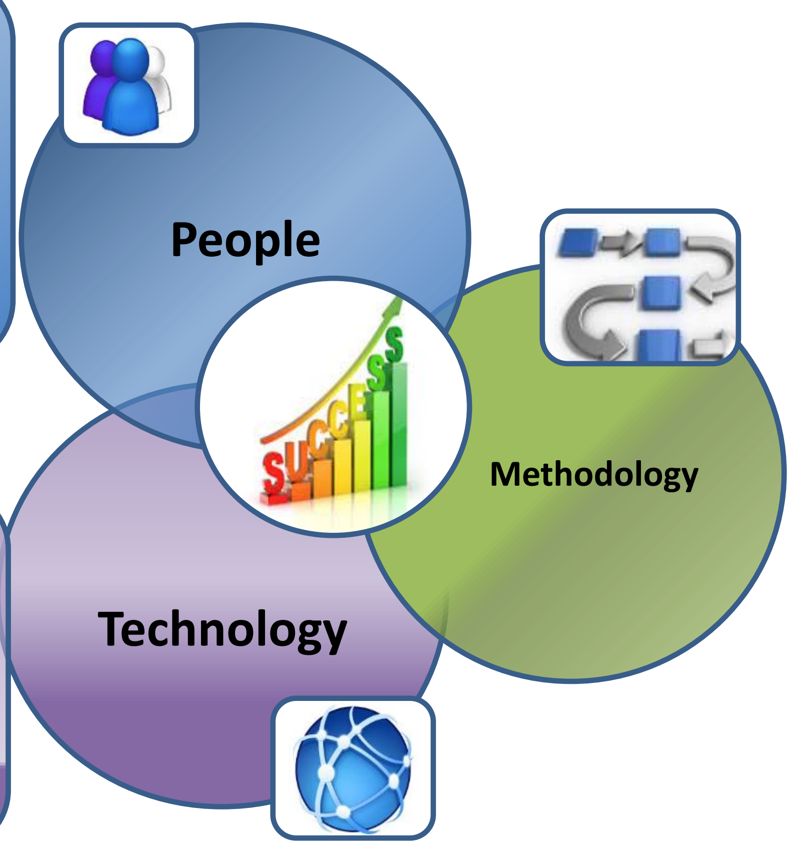
Cyber Defense

Team

Intelligence

How to defend your organization

- Staff & Training Awareness
- Professional Skills & Qualification
- Competent Resources
- Use Red team, Pen Tests

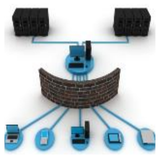


- Operational tools & methodologies
- Management Systems
- Set and monitor quality standards and controls
- Break the Routine

- Orchestrated Tools and Inter.
- Cannot deploy technology without high level resource and good Methodology

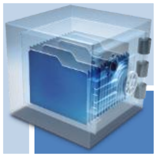
Vectors of Solution

Regulation and Compliance



External

- **Risk Based Authentication & Authorization**
- DDOS
- Mobile Security
- Secure Code (and SSDLC) for mobile Apps
- Bid data analysis for abnormal behavior

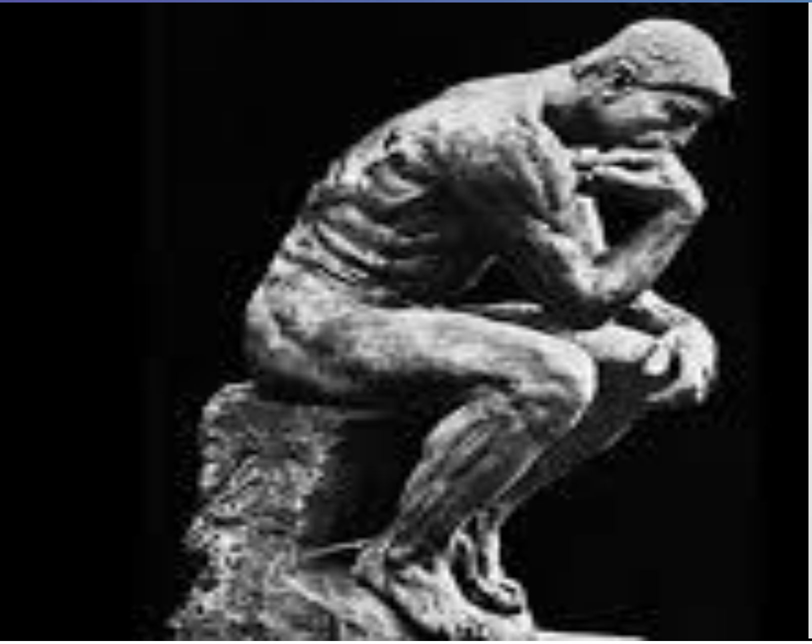


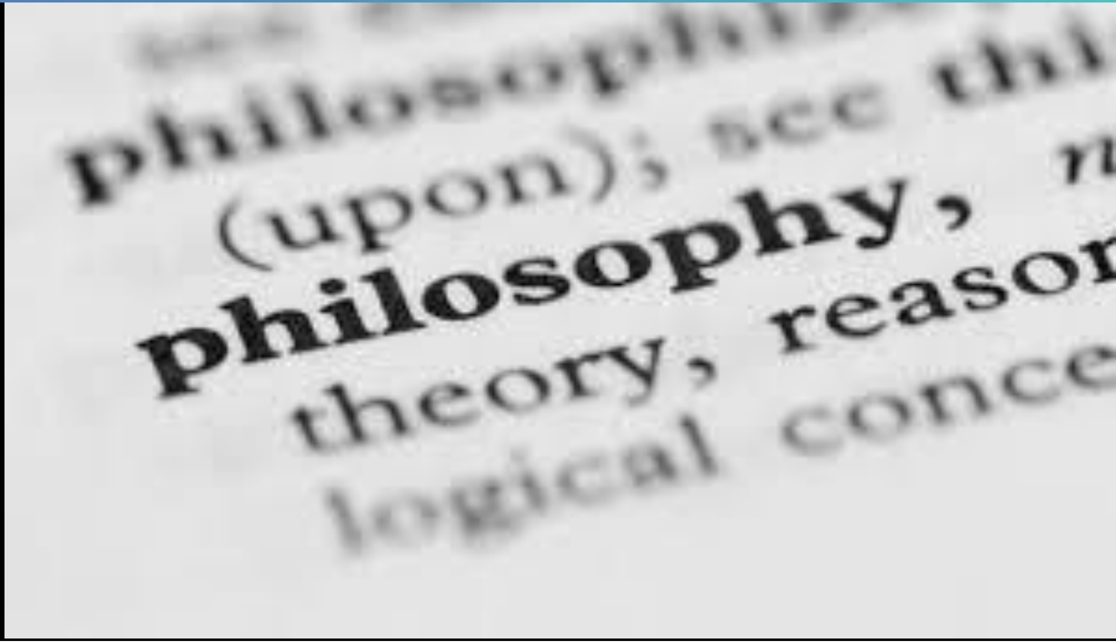
Internal

- **Cloud Security (Privet & Public)**
- SIEM/ SOC
- Sensors
- Big data analytics
- NFAT
- Forensics Tools & methodologies
- Advanced EPS
- Cyber Intelligence
- Compliance
- Training & Education

Partners

- **Supply Chain survey**
- Cyber Security Instruction and Requirements
- API Gateway





Our Philosophy

Our Philosophy

There are many multi billion cyber security companies

Yet … the cyber problem is an open issue

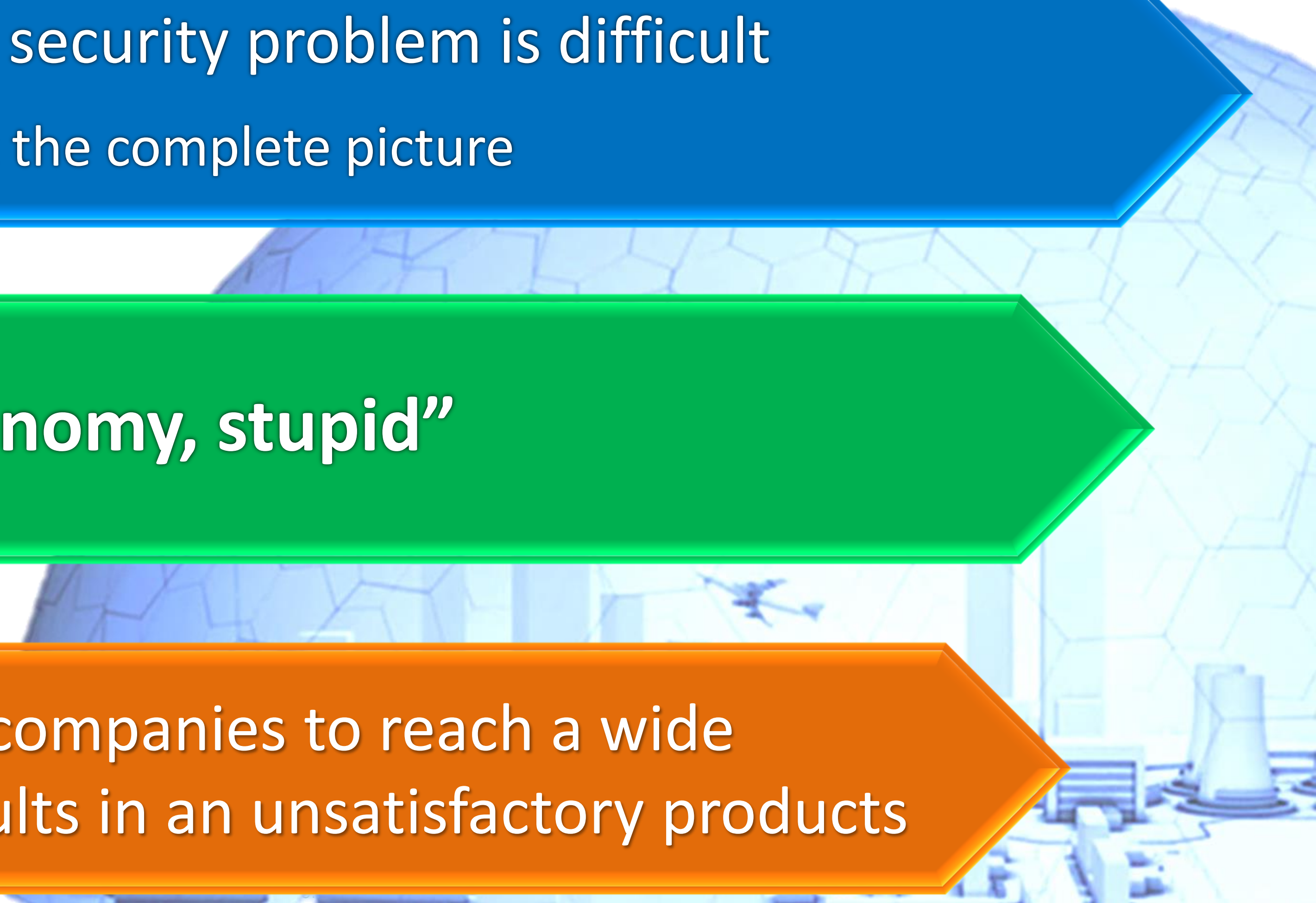
There are many established commercial cyber products

Yet … the cyber problem is an open issue

There are many startups funded by venture capital

Yet … the cyber problem is an open issue

So, what's the problem???



Yes, the cyber security problem is difficult

- But that's not the complete picture

"It's the economy, stupid"

The effort by companies to reach a wide audience, results in an unsatisfactory products

There are many cyber solutions and products

Yet … the Cyber challenge is an open issue

The solution should be tailored to the customer needs, environment and ecosystem

Cyber Defense

Summary

- The Cybernetic **already** met the Physical
- **Surprise** is mandatory
- We must be ready and keep **Business Continuity**
- **Tailored** solution to the customer needs, environment & ecosystem
- **Change from** :
  - Product to Solution
  - Cyber **Security** to Cyber **Defense**

Questions?????

Thank You!