Cybersecurity
When the time is over…

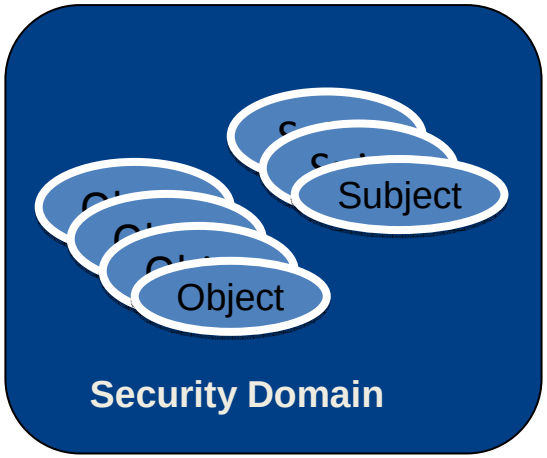
Practical guide : « Deploying defensive cyber warfare measures and Policies in a Critical Infrastructure Sector »

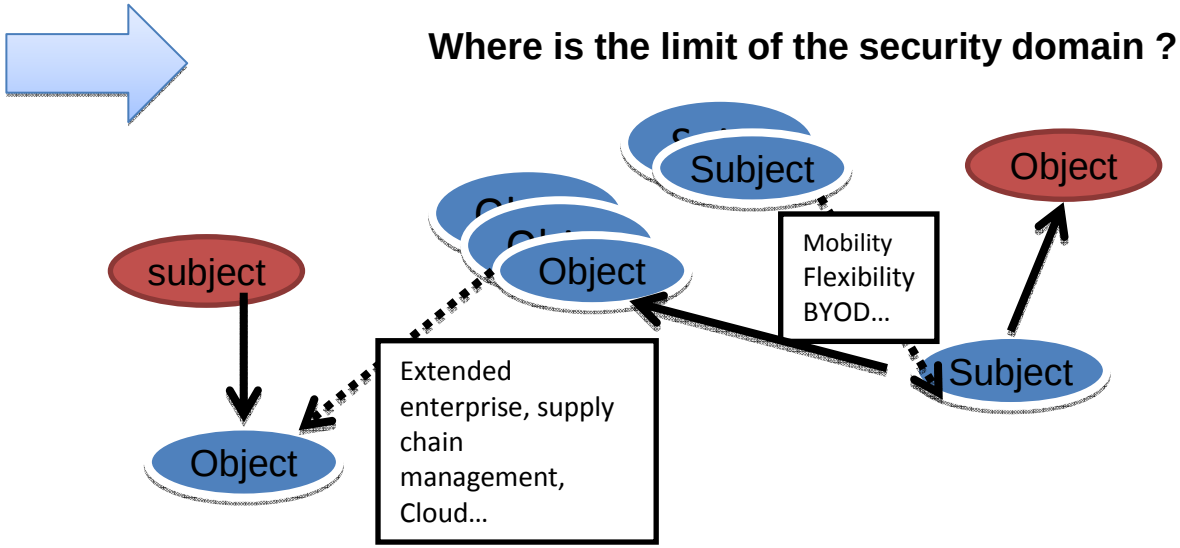
Sébastien Bombal
Insomni'Hack 2014

Introduction - We all know this story…

- Critical Infrastructure, Building management systems, Internet of things, Industrial SCADA systems… always the same :
  - Security design and hardening issue
  - Highly connected
  - Embedded management, high availability concerns
  - Obsolescence management is a nightmare
  - Engineer without training and even awareness of cybersecurity basics
  - ….
- But just remember the past – same story some years ago with
  - Printer to Multifunction devices evolutions, Telephony to VoIP / IPBX transformations, …
- And finally the same root causes of issues/vulnerabilities for new technologies ?
  - Mobile phone to smartphone, …
- Is there a difference ?
  - “Just” a direct link from virtual to reality
- And most of the solution is already known to counter this ...
  - Stop to rediscover the rainbow books ☺

Defense in depth of course ! But where is the border ?





And threats are more and more aggressive…

While the market has evolved in the opposite directions

Security based on discretionary mechanism…

Non deterministic systems…

Detection and reaction are the poor relation of Cybersecurity…

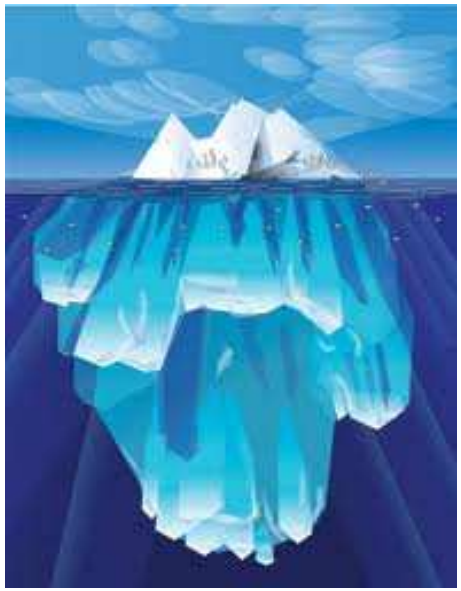
Organization focus on physical security and compliance …

Forgotten basics and histories…

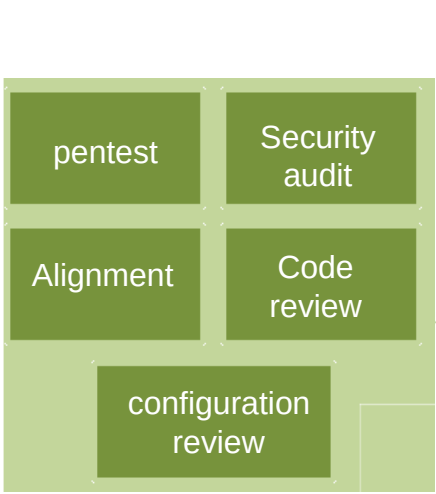
Market must be able to address the new stakes

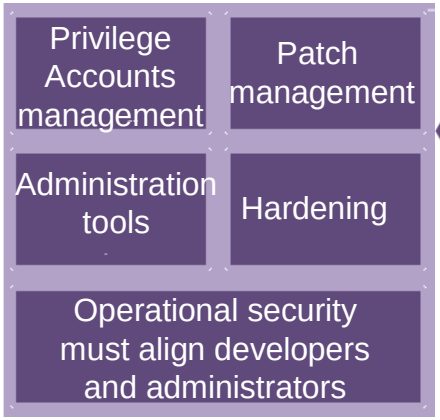
Face to the issue ? How to defend the IS ?

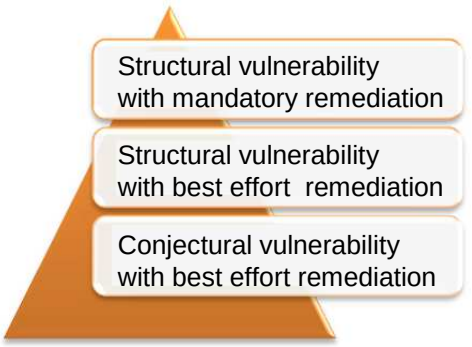
Sponsorship ?	• Security do not stop with IS organization • Completeness of the scope (IT and OT / Operations Technology) is the key
Organization ?	Deployed exhaustively Cybersecurity on BUILD and RUN processes for IT and OT
Maturity level ?	• Audit : in order to know your IS, to protect or enforce it, before finally delay or even contain a cyber-attack • Detect / React : Learn from incidents
Technology ?	• Applied Cybersecurity basics – Yes it's possible • Transform your IS in a deterministic one in order to detect weak signal and to suppress noise in logs • Know in details your IS and technologies
Market ?	Quite difficult right now….



Defend an IS means first to enforce it…

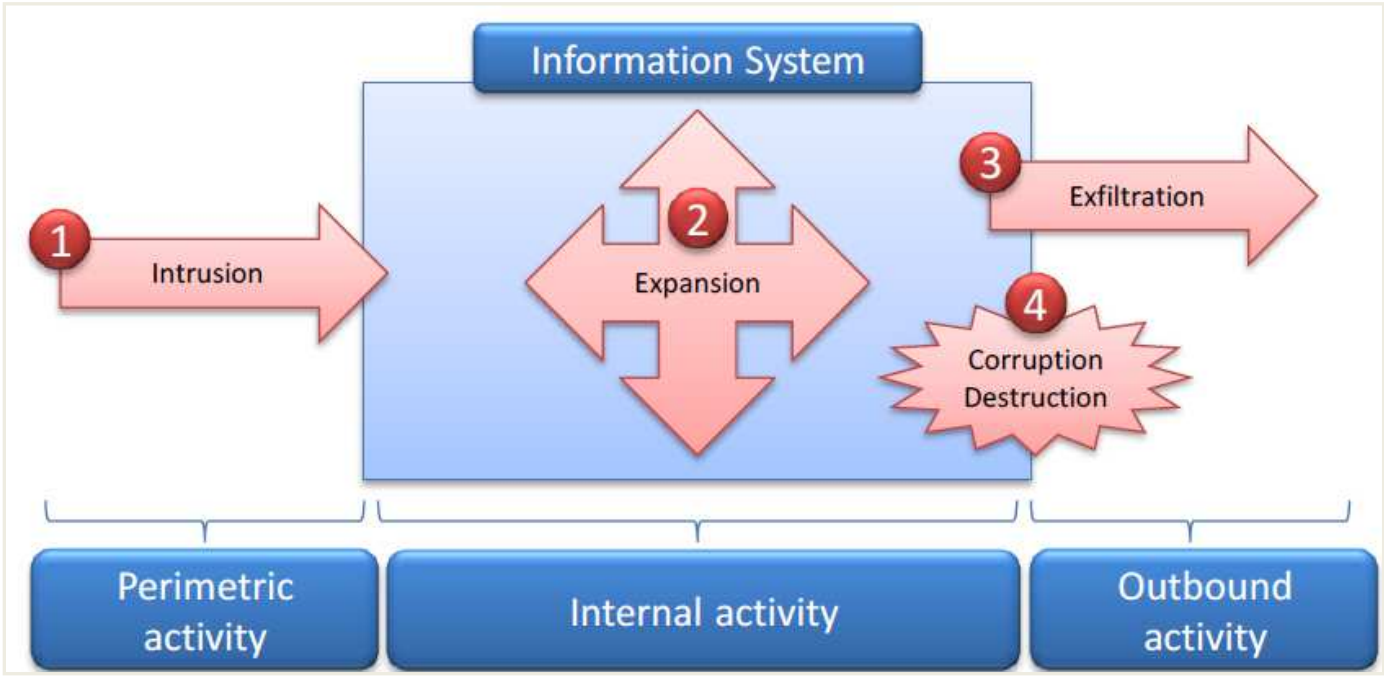






- A DMZ is not a proxy
- Mutualize and consolidate without multilevel security issue
- Security design from end to end (administration, monitoring or backup tools without breaking the security zoning

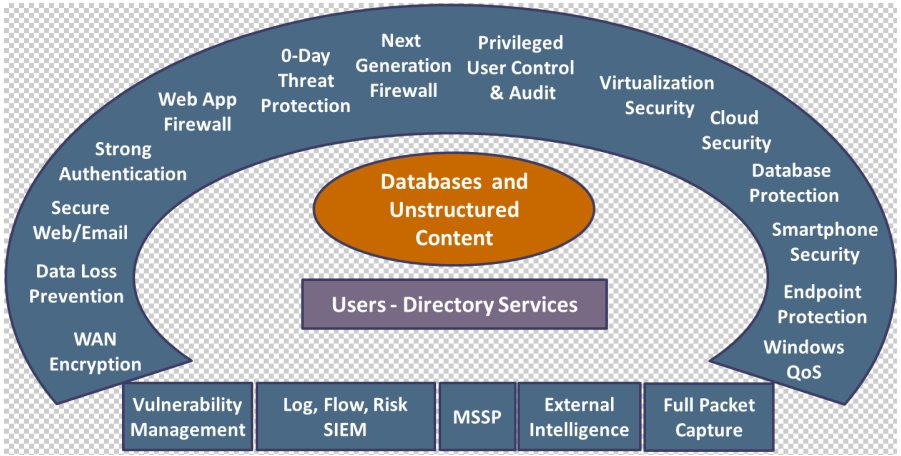
And to endue with detection and reaction capability



Intrusion is unavoidable – you cannot protect everything …	Vertical and horizontal expansion can reach the point, with irreversible consequences Step 2 is The critical step to deal with !	Learn to temporary accept situation to get it under control

Do not stake all your security on protection…

But this is what the market sells – with security model based on “black list”



Everything to secure but not to defend !

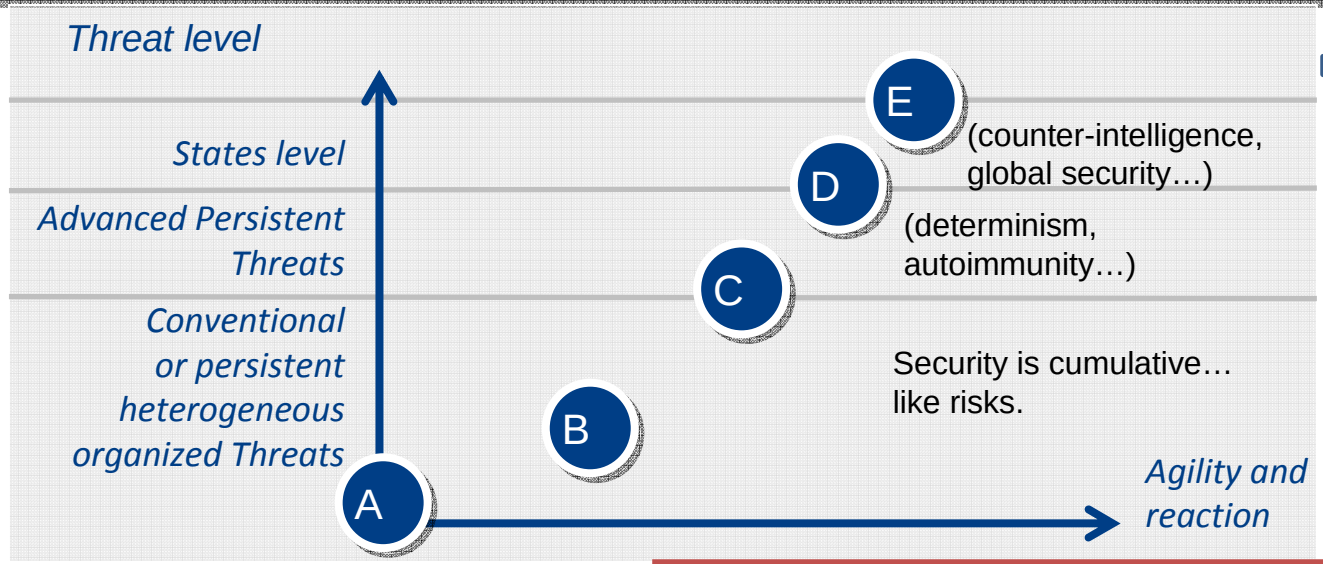
Head of the Cisco Computer Security Incident Response Team *“If anyone attempts to sell your organization on a hardware or software solution for APT, they either don’t understand APT, don’t really understand how computers work, or are lying – or possibly all three.”*
http://blogs.cisco.com/security/cisco-csirt-on-advanced-persistent-threat

Defense in depth is necessary
And theoretical model must evolve (proposal in red)

	Preventive Protection Investigation	corrective	Detection & Reaction	deterrent	recovery & resiliency	compensation
Physical			Case of ARAMCO		BCP / DRP	
Logical						
Administrative						

But this defense in depth strategy can only respond to risk analysis or audit reports or incident REX

Maturity & Defensive Cyber Warfare



And what if our work was to measure time and to optimize time ?

KPI cyberdefense ?

- **A** Manual and reactive
- **B** Tools oriented
- **C** Agile and mature
- **D** Dynamic defense
- **E** Resiliency

Let A be the interval for time, $A = [0 ; +\infty[$

Let $x \in A$ be x = Time $_{\text{to compromise an IS up to an unbearable point}}$

Let $\bar{X} \in A$ be the lowest value for = Time $_{\text{of detection}}$ + Time $_{\text{of reaction}}$ + Time $_{\text{to stop or contain}}$

1. A system can be considered well-defended if $\bar{X} \in [0, "x"[$
2. A system can be considered badly defended if $\bar{X} \in ["x", " + \infty"[$

$\exists f$, an optimization function "objective / criterion", empiric, non-linear, depending of the system, and should content:

- A resistance coefficient of the IS
- A constant linked to the incompressible delay of detection
- A variable linked to the knowledge and training of the defending teams
- A variable linked to the knowledge and expertise of the attacking teams

How to measure ? Audit Red Team or crisis REX

And after all, the incident arises…

Source of launching ?

- Strong signals ➔ SOC / SIEM / CERT…
- Weak signals ➔ Organizational detection thanks to the knowledge of the behavior of the IS

Organization to cope the crisis

(back of the organization = defense plan)

1. Audit : the scope concerned (identify potential vulnerabilities in order to feed the defense plan)
2. Investigate (live or post-mortem) and feed again the team of the defense plan
3. Prepare the D-Day to this control tightening (roll out defense plan)
4. Manage stockholders (management, authorities, customers, external communications…)

Defense plan

1. Measures before the D-Day
2. Measures during the D-Day
3. Measures after the D-Day

The D-Day

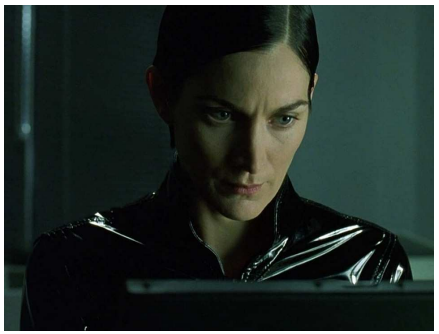
- Success is linked to the human resources management

After the D-Day

- Be prepared for impacts management
- Be prepared for resources management
- Roll out security measures post D-Day
- Be prepared to answer to a lot of questions… (customers, authorities, press, ….)

Which are critical success factors ?

- Short decision cycle and sponsorship at the right level
  - It's a crisis process and not a project management !
- Confidentiality of the operation but be ready to communicate at anytime (internally and externally)
  - Confidentiality is a tactical advantage



- Build a incident response team with the appropriate size
  - A cyber attack can keep on many weeks and months before to regain full control
  - Necessity to leverage resources, and in the worst case to double IT teams (one for the RUN, one to BUILD a completely new IT…)
  - The key is in the human resources management (on duty, non business hours, vacancies, turnover……)
- Be able to unfold the defense plan at anytime even without an exhaustive vision
  - "Non exhaustive" : you will have to leap to the attack and you will always have good reason to delay the D-Day
  - "At anytime" : if the assailant discover your operations or reach the unacceptable point
  - Strategy of "technical harassment" on assailant can help you to play for time
- Track all of your decisions and acts, since you will have to answer for them for a long time…

Finally – go over your perceptions on Cybersecurity

- About awareness
  - Priority is on the high privileged accounts for OT and IT
  - Effectiveness on end users is highly debatable.

- An organizational security measure does not achieve anything without technical security measures… but …
  a good technical security measure will be not applicable without organizational measures

- Having breakpoint (like in negotiation) on projects or run activities
  - A software editors who produce without least privileged or defense in depth principles ?
  - Financial performance objective that imply to consolidate / mutualize and create multilevel security issue ?
  - Unsecured outsourcing or interconnections with partners with only a contract ?
    - Contracts protect legally but do not defend your IS

- Devil are in the details – come back to the technique !

- Crisis is not a fatality, if you turn it into opportunity

Thanks for your attention !