Cybersecurity and railway signalling

27 May 2014

Technology Platforms

In the Past	Today
✓ Proprietary HW/SW ✓ Isolated Systems ✓ Dedicated Applications ✓ Structured Information	✓ Commercial low cost HW/SW ✓ TCP/IP Protocol ✓ Interconnected Systems ✓ Heterogeneous Services (E-mail, Info-web, VoIP, CCTV, …) ✓ Structured and unstructured Information

Operating Environment

Today
✓ Distributed ICT infrastructure spread over long distances, and unattended systems
✓ Connections between safety critical and non-safety critical layers
✓ External systems connected to signaling infrastructure
✓ Human factor (operators, maintainers and… passengers)

Cyber Space calling, Cyber Security knocking

Cyber Security: protection of Cyber Space. But what is Cyber Space?

Yesterday: many different environments, side-by-side

Today: one single, big environment

Consequences: Dynamic Threat Landscape in unique Cyber Domain		
Strategic & Tactical Cyber War	Military	Stuxnet, Operation Aurora, Botnets
Terrorism	Politics	
Espionage	Intellectual Property	Zeus, Flame, APT AET attacks, Botnets, Phishing e-mail
Organized Crime	$	
Vandalism & Hacktivism	Ego, Curiosity	DDoS attacks, Wikileaks, Anonymous

ICT Security Governance

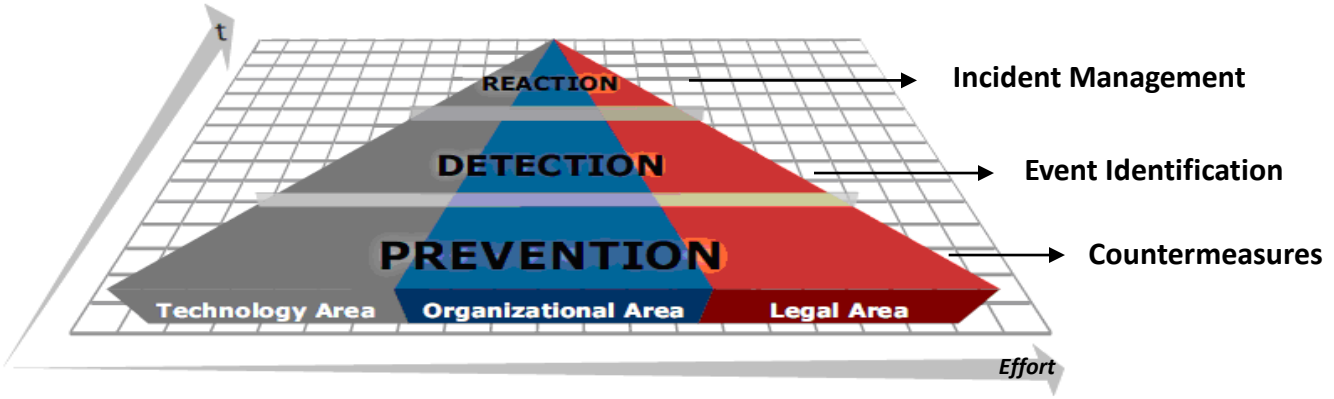
A) Security Goals: Data Confidentiality, Integrity and Availability (ISO27001)

B) Sequential activities:

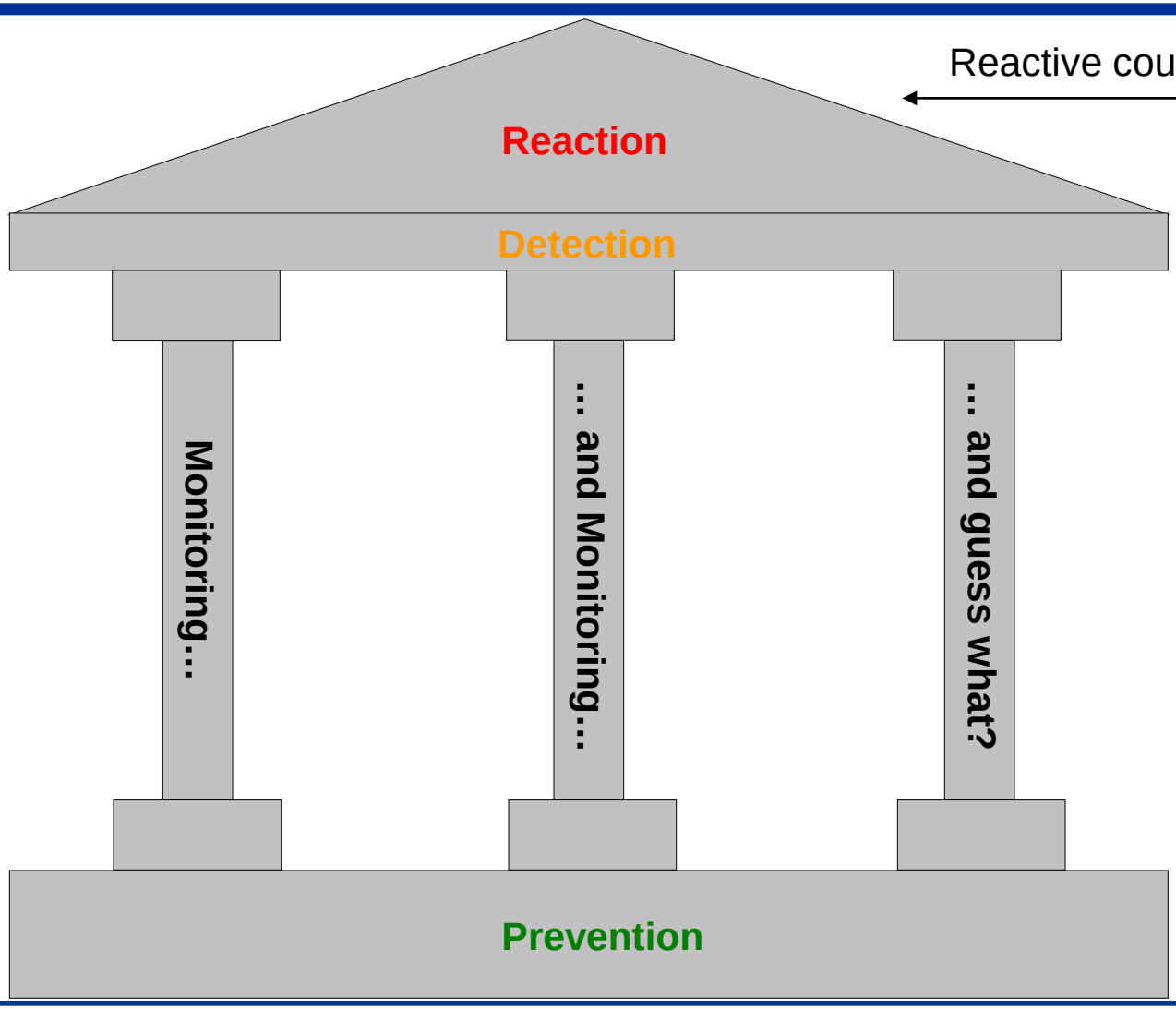
- PREVENTION: Preventing information violations by countermeasures
- DETECTION: Identifying and Monitoring/Reporting events when they occur
- REACTION: Developing strategies & procedures for incident management

C) Information Security Management System (ISMS) composed by:

- TECHNOLOGY AREA
- ORGANIZATIONAL AREA
- LEGAL AREA



ICT Security Activities and Governance: real life



Reactive countermeasures

WTF is goin' on???

(not excluding Forensics)

Proactive countermeasures

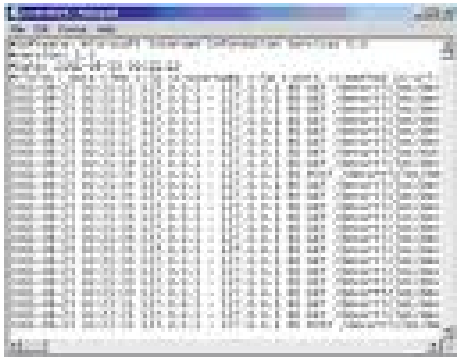
Strategy: enhance monitoring and correlate

Firewalling

Content Filtering
Virtual Patching

IDS/IPS

AAA



So many eyes… giving a very broad view (say, at 365° degrees… to stay safe)… OK…

But where to look for? And for what? And who?

Cyber Security: taking advantage of IT

Building on top of Information Technology infrastructures, means that you get both its weaknesses, true, but its strenghts as well…

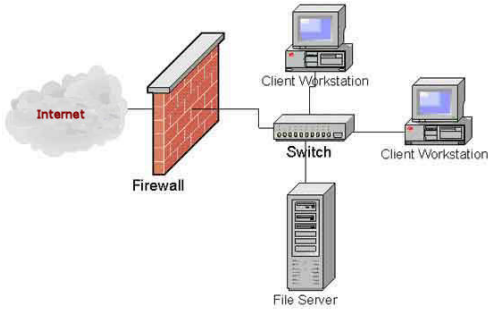
… putting it the other way round: if a system is not secure by design – and they are not –, it will leave plenty of traces for you to follow!

Leaving trace-routes behind

Perimeter Defence – Cyber Security policies

White Listing: *only* **allow** *explicitely listed traffic*

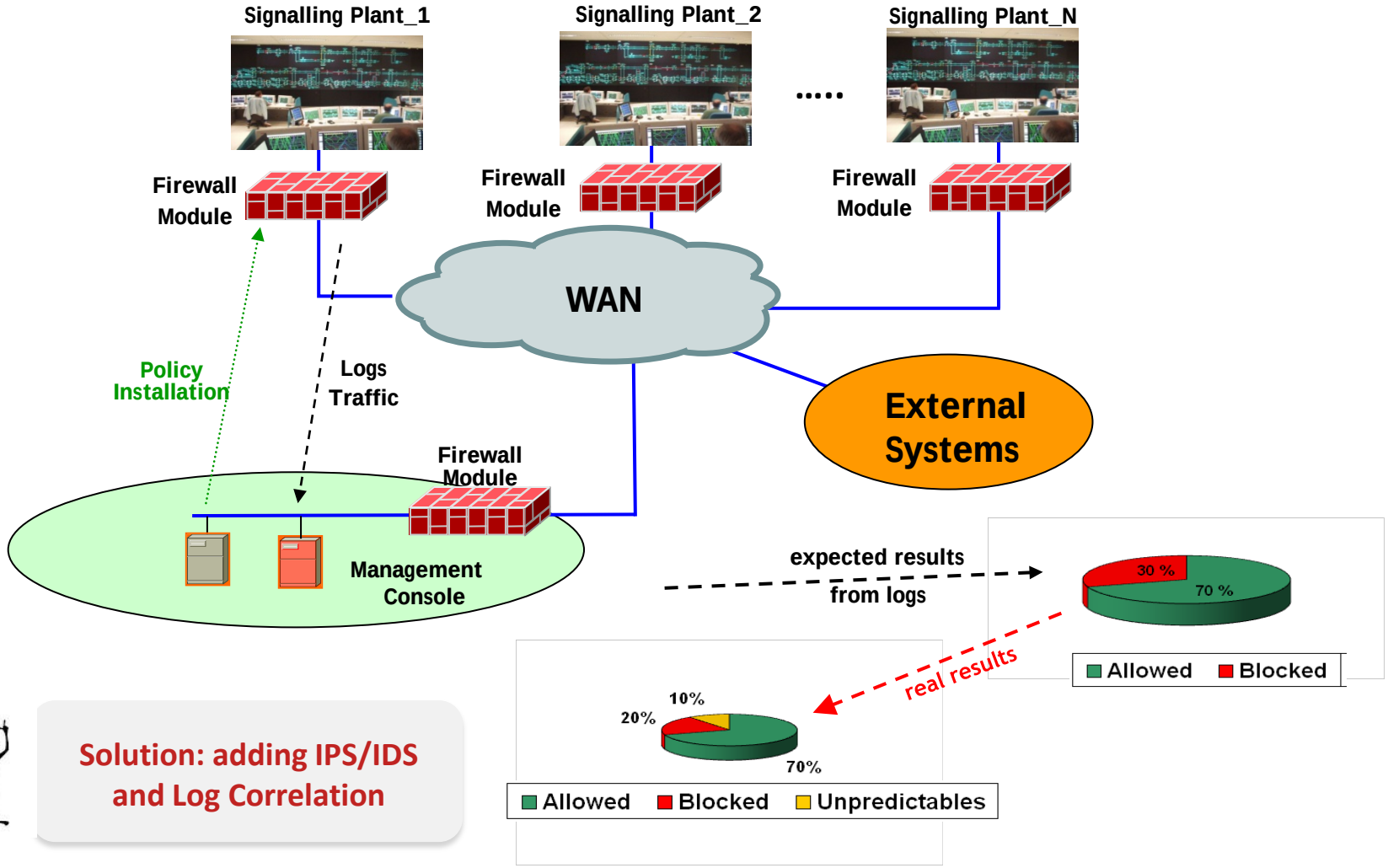
(and as a corollary: whateverelse is forbidden)



Black Listing: *only* **deny** *explicitly listed traffic*

(and as a corollary: whateverelse can go thru)

Perimeter Defence - Firewall shortcoming



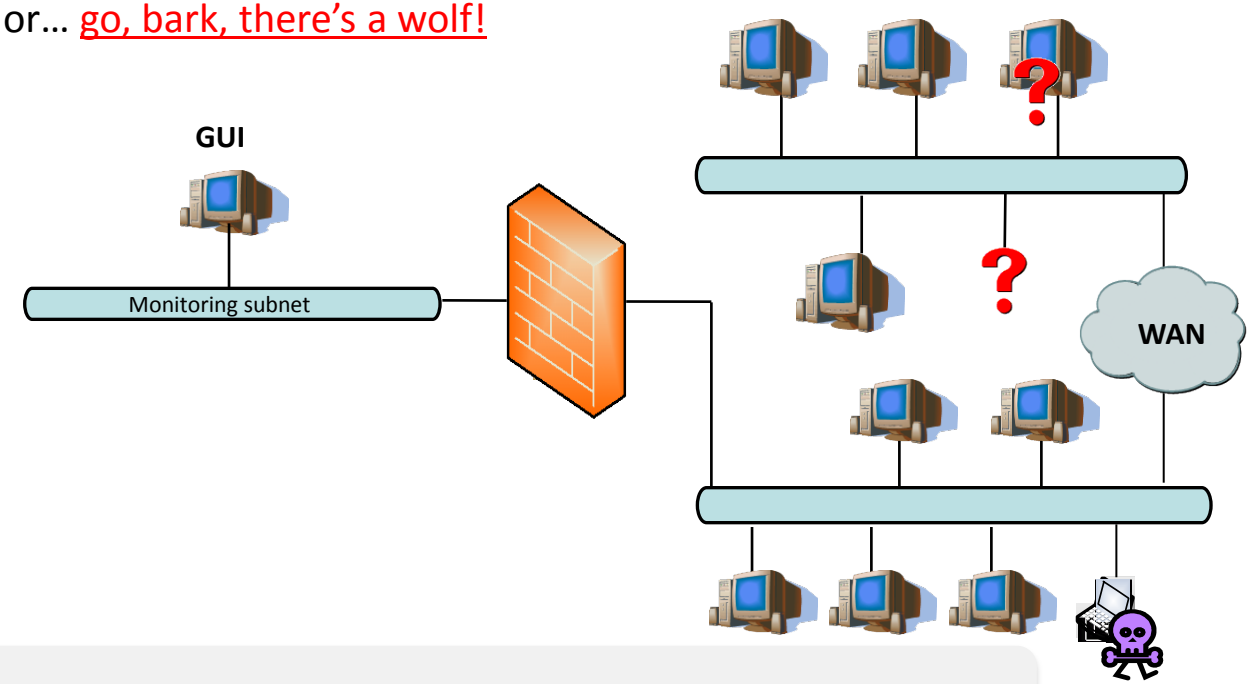
Solution: adding IPS/IDS and Log Correlation

Near Realtime Asset Control

- not a performance- or availability-driven tool, though it may help
- based on static asset database loaded offline at project time
  - perform differential discovery onsite for database tuning
  - acknowledge variations that should be allowed
  - what is left, deal with: either a missing sheep, or a mismatched one,

or… go, bark, there's a wolf!

Repeat as needed



Know your flock, and beware of wolves! Barkin', at the very least

The russian peasant of SIEMs at work: fast and light

LOG CORRELATION

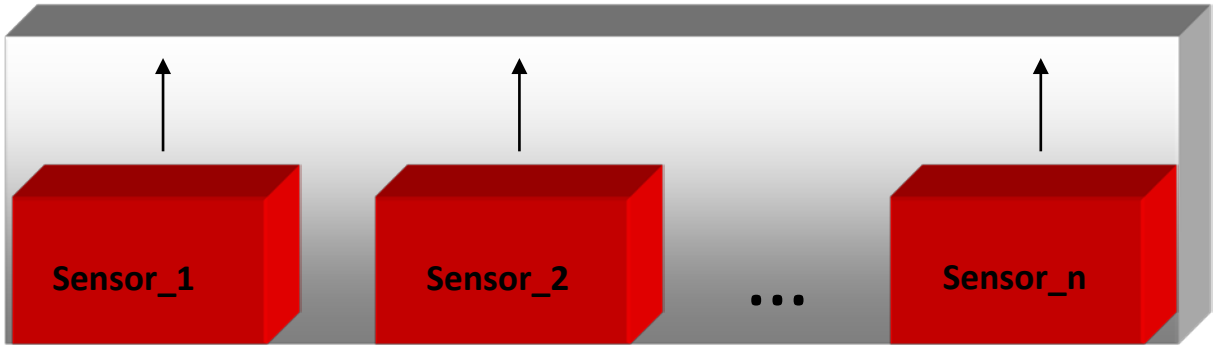
Events Console

Correlation Engine

Message Correlation

- Minimize False Positives
- Realtime response (no archiving)
- Novelty detection for scheme-in-the-chaos

Log Files



The 11th hour (a.m.?)

Do we simply wait for vulnerabilities to become actual threats

or

Can we advance from here, and provide for new services?

Cyber Security = Defense line