encode
Information Risk Management

Innovating Security with
Big Data Analytics…and Attacker TTPs

Panos Dimitriou, CTO

InfoCom Security 2013

Advanced Cyber Threat Management Services

Audience

If you are an Organization that does NOT:

- Have specific unique information assets (e.g. Intellectual Property)
- Have competitors (or opponents) that can gain an advantage by obtaining access to internal, confidential information of yours
- Provide the opportunity to criminals for direct/indirect financial gain, by acquiring access to your data/services
- Manages Critical Information or Critical Infrastructures
- Have customers (and access to corresponding data) that belong to the above criteria

Then you don't care about handling Targeted Cyber Threats…and this presentation

Security Facts

- Targeted Cyber Attacks have shed light on the actual effectiveness of the current Security (Prevention/Compliance-oriented) Paradigms

- **The outcome: “The Emperor is naked!”**

- The “APT” and especially the “Advanced” nature of the Threat rattling is used as an excuse for security failures

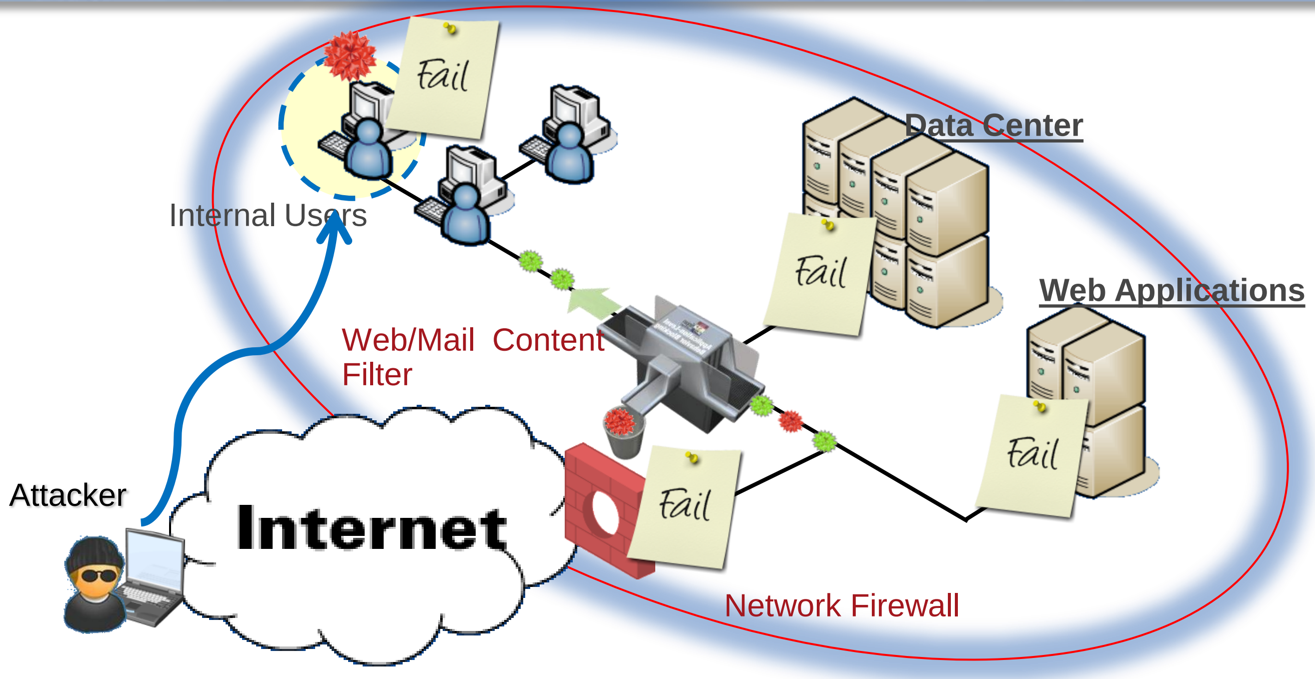
- The fact is:
  - The threat is very real
  - It’s not the threat that is advanced
  - It is our current Security paradigms and corresponding Tactics, Techniques & Procedures that are misfit… and totally predictable

encode
Information Risk Management

Targeted Cyber Threats aka. APT

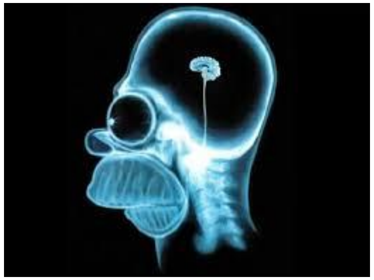
Today adversaries run persistent attack campaigns against specific targets

Common techniques cover targeting the end user - taking control of its workstation bypassing all commonly used security technologies

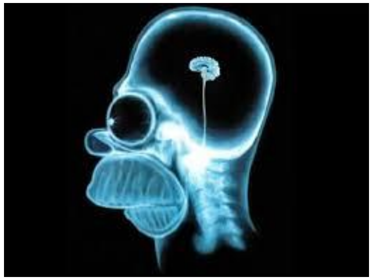


These threats are referred as Targeted Cyber Threats or **Advanced Persistent Threats (APT)**

Malware Problem vs. Targeted Cyber Attack/APT Problem

Threat	"Intelligence" Level	Scope & Objectives
 Malware Infection - Autonomous/Automated	 "basic survival instincts"	 Endpoint – local data, Financial Fraud…
 APT – Remote Access Tool/Foothold	 Human Operator/ Hacker	 IT environment – Data exfiltration, sabotage, fraud…

Malware Problem vs. Targeted Cyber Attack/APT Problem

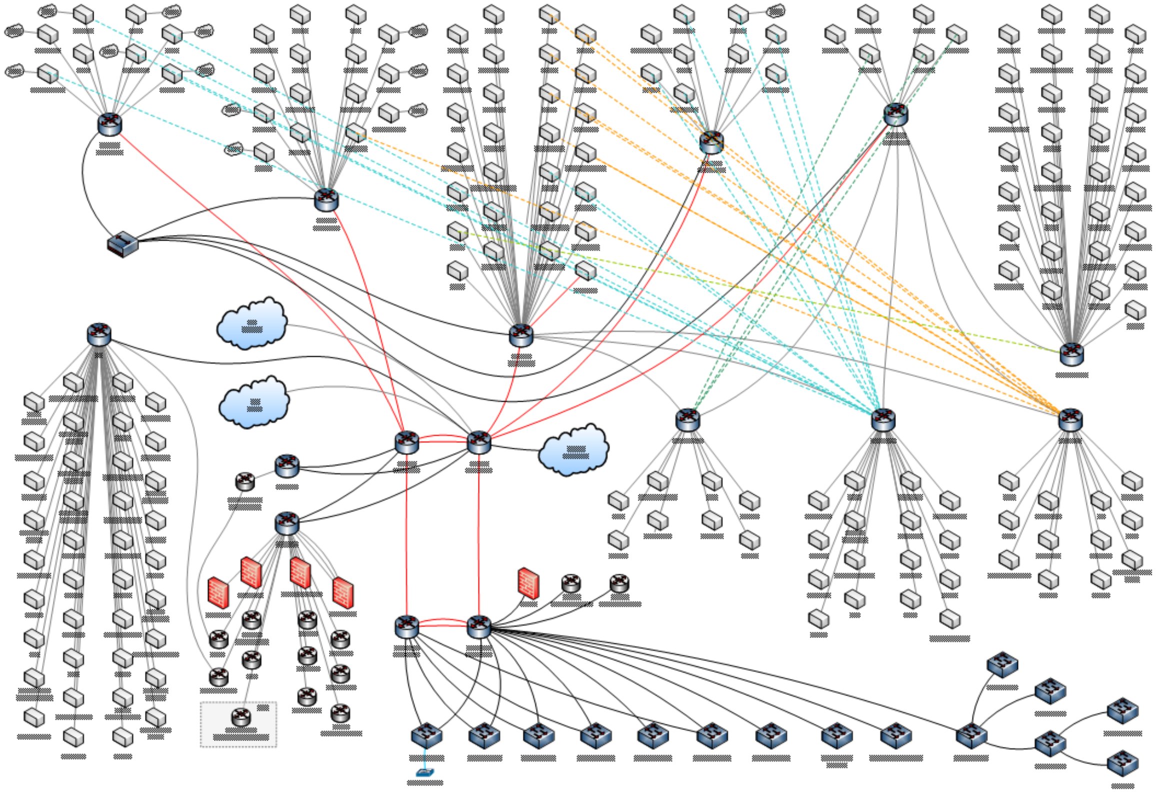
Threat	“Intelligence” Level	Current Defenses	“Intelligence” Level
Malware Infection - Autonomous/Automated	 “basic survival instincts”	FW, AV, IPS, SxG… - Autonomous/Automated	“ameba”
APT – Remote Access Tool/Foothold	Human Operator/ Hacker	FW, AV, IPS, SxG… - Autonomous/Automated	“ameba”

We have already a mismatch

The APT "Breach Game"

They have to compromise this

Advantage



You have to defend this

Challenge

and the mismatch goes on…

encode
Information Risk Management

The APT "Breach Game": Your Opponent…or Adversary

They are:

- knowledgeable
- well trained
- well sourced
- persistent
- mobile
- adaptable
- agile
- swift

They will:

- Profile/Recon
- Deceive
- Evade
- Infiltrate
- Escalate
- Persist
- Adapt

The APT "Breach Game": You … a sitting duck

The perfect mismatch

You are:

- knowledgeable
- well trained

…but also

- Understaffed
- Underequipped
- Under-budgeted
- Overwhelmed
- Reactive
- Unmoving

You try to:

- Prevent
- Respond
- Remediate

…

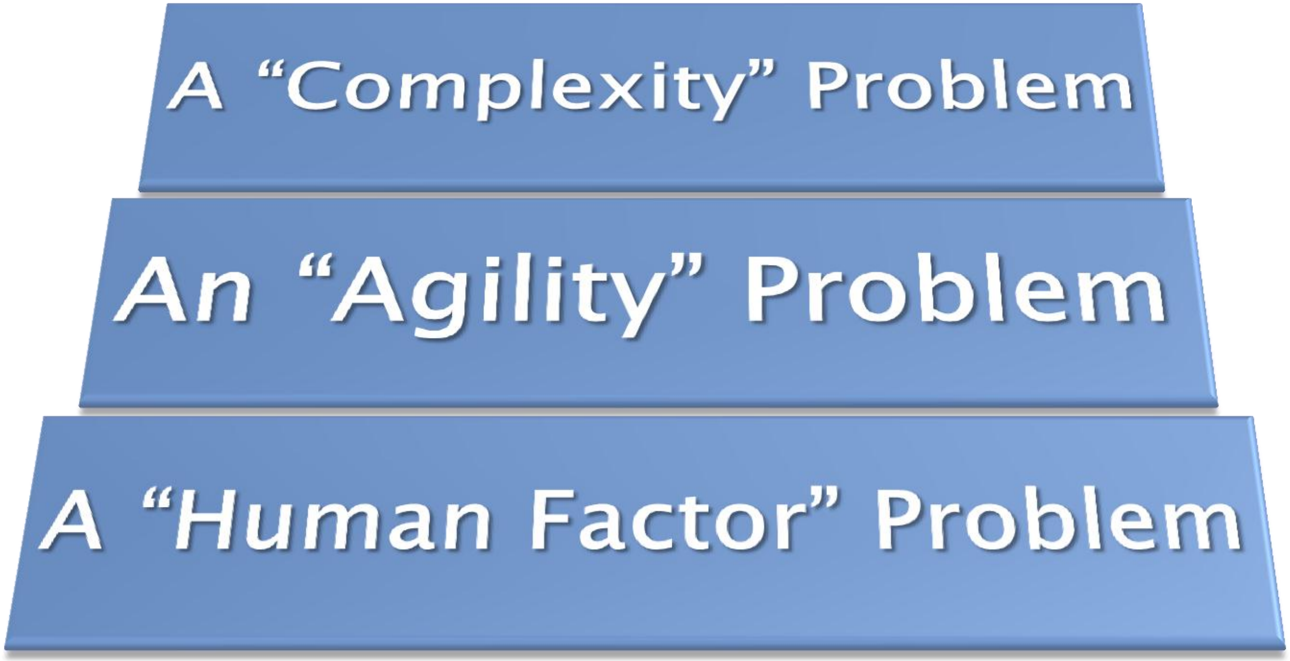
- Be Compliant
- Be in budget
- Be on Time

encode Information Risk Management

Innovating Security with Big Data Analytics & Attacker TTPs

Redefining the APT Problem

We believe it is 3-fold problem:

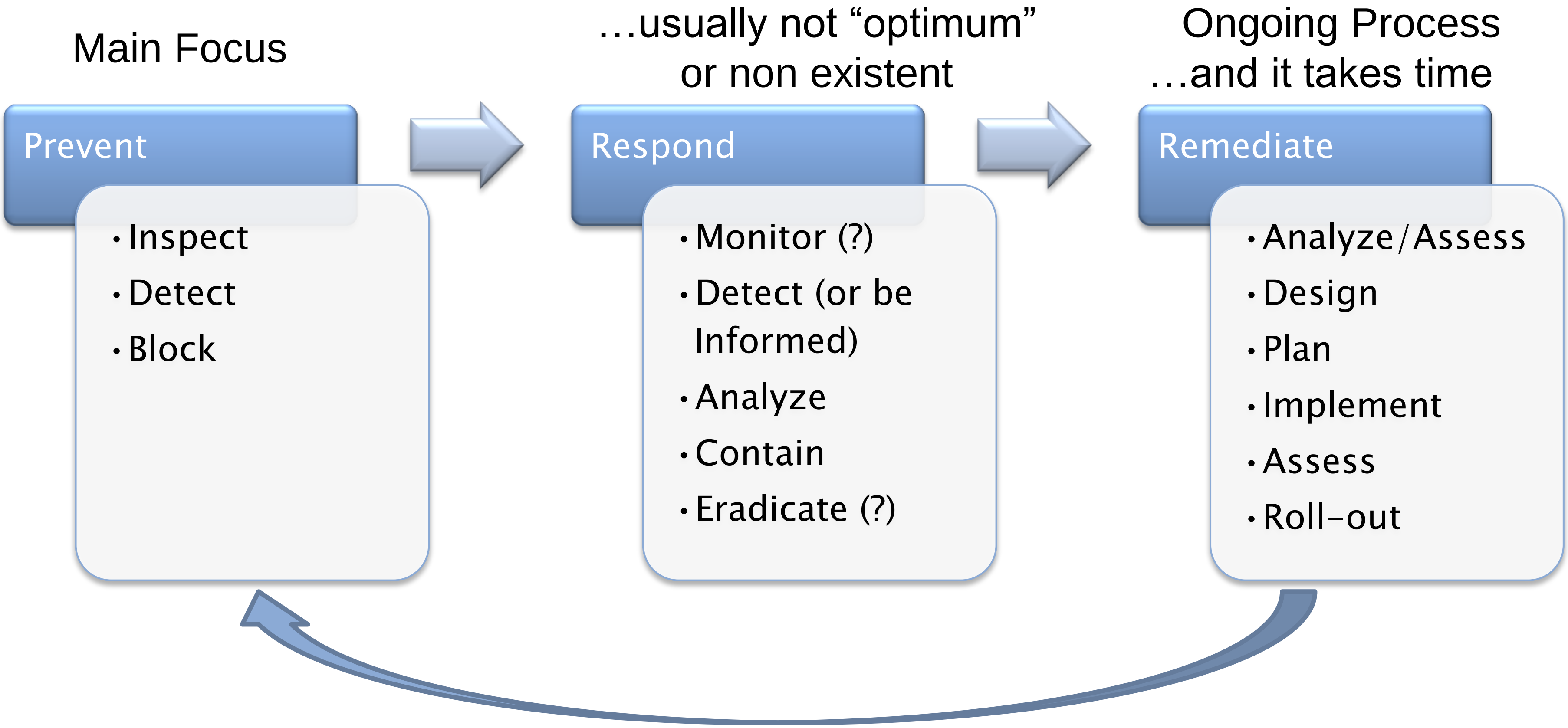


A "Complexity" Problem

An "Agility" Problem

A "Human Factor" Problem

Current Cyber Security Defense TTPs



Main Focus

Prevent

- Inspect
- Detect
- Block

…usually not "optimum" or non existent

Respond

- Monitor (?)
- Detect (or be Informed)
- Analyze
- Contain
- Eradicate (?)

Ongoing Process …and it takes time

Remediate

- Analyze/Assess
- Design
- Plan
- Implement
- Assess
- Roll-out

encode Information Risk Management

…don't expect to "win" with this!

Learning from the Attacker’s TTPs …and Sun Tzu

- **Profile – *“If you know the enemy and know yourself…”***
  - Continuous modeling of your IT environment
  - Internet Access, Endpoint Activity, Intranet Access…
  - Building statistical models & Measuring Deviations
  - Detecting Generic Threat Patterns, based on attacker’s TTPs
  - Calculating “Threat Scores” by combing the two (Deviations + Patterns)

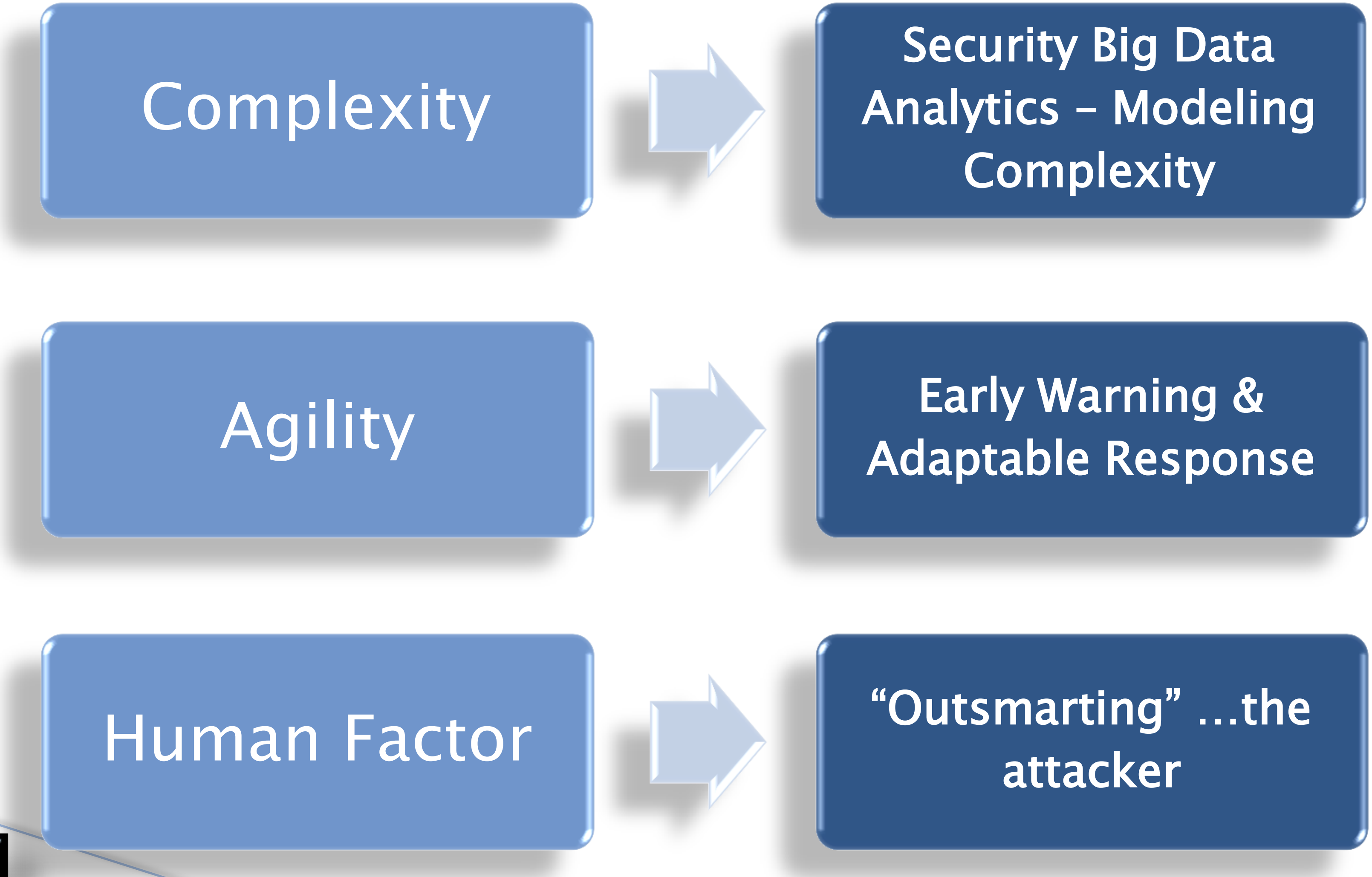
- **Adapt – *“Move swift as the wind…”***
  - Adapt your responses according to the “Threat Score”
  - Automatically Inspect suspicious Endpoint Activity
  - Mobilize your Security experts to analyze suspicious activity
  - “Stealthily” Contain & Monitor a confirmed incident/attack under way
  - Eradicate the threat only when you have a complete picture…and before having a (serious) impact

ART OF DECEPTION

- **Deceive – *“Engage people with what they expect…”***
  - Turn your “weaknesses” to “advantages”
  - “Give an end-user an endpoint and he will never fail to get compromised” (or “owned” in the hacking terminology)
  - “Give an attacker (plausible) “low hanging fruits” and he will never fail to grab them”

encode
Information Risk Management

Solving the APT Problem



Complexity → Security Big Data Analytics – Modeling Complexity

Agility → Early Warning & Adaptable Response

Human Factor → “Outsmarting” …the attacker

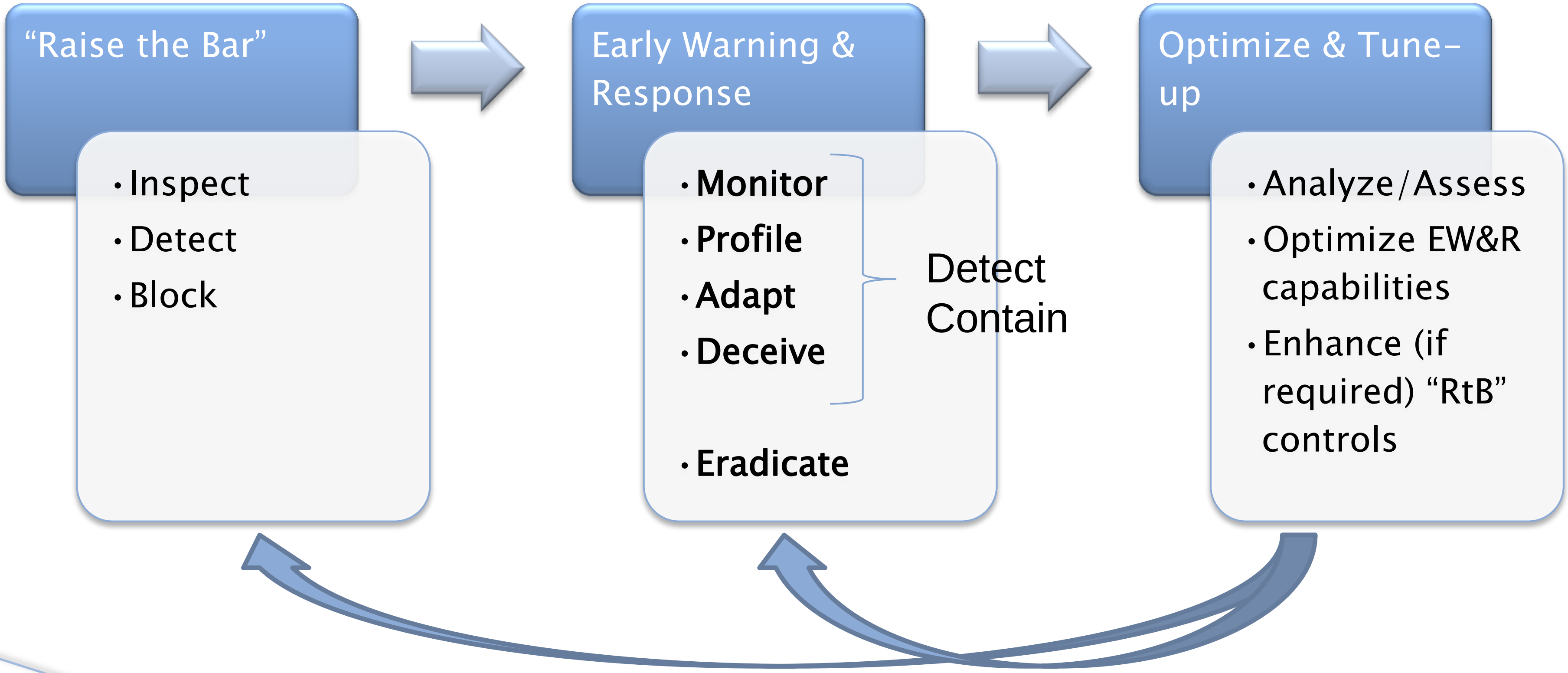
encode
Information Risk Management

Redefining your Cyber Strategy

It is not Prevention… it is just "Raising the Bar"

Main Focus

Ongoing Process



"Raise the Bar"

- Inspect
- Detect
- Block

Early Warning & Response

- **Monitor**
- **Profile**
- **Adapt**
- **Deceive**

Detect
Contain

- **Eradicate**

Optimize & Tune–up

- Analyze/Assess
- Optimize EW&R capabilities
- Enhance (if required) "RtB" controls

"Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat." - Sun Tzu, The Art of War

Questions & Answers

Answer#1 : NO, YOUR SIEM CANNOT DO THIS

encode

securing the future of e-business

www.encodegroup.com_