SECURITY MATTERS

TU/e Technische Universiteit Eindhoven University of Technology

Where innovation starts

Network Monitoring of Industrial Control Systems: the lessons of SecurityMatters

A position paper & presentation

Partly based on the 2017 ESORIC invited talk “From Intrusion Detection to Software Design” (but my opinions have become slightly more “radical” since then)

Sandro Etalle

Why me

- Worked on Intrusion Detection,

- First in academia
- Then, in our spin-off
  - CEO for 4 years+
  - I talked to customers
  - and learned a few things

- SecurityMatters
  - The “first” company in the space of network monitoring of Industrial Control Sysems

SecurityMatters: the start

- 2005-2006. Three Italians in Twente
- Goal: change intrusion detection
- We wanted to make anomaly detection for intrusion detection finally work

- We were not the first ones to try:

- *"… despite extensive academic research one finds a striking gap in terms of actual deployments of such systems… "*
  Robin Sommer, Vern Paxson: S&P 2010
- Several bankrupt companies (we didn't know)
- Proving again that foolishness can be key…

The story in a nutshell

2005: Research

2009: Company established in Twente

2012: 12 people, live pilots

2013: First customers (USA & NL)

SecurityMatters LLC (USA) incorporated

2014:

- moved to Eindhoven
- Gartner CoolVendor
- Market & competition arrives

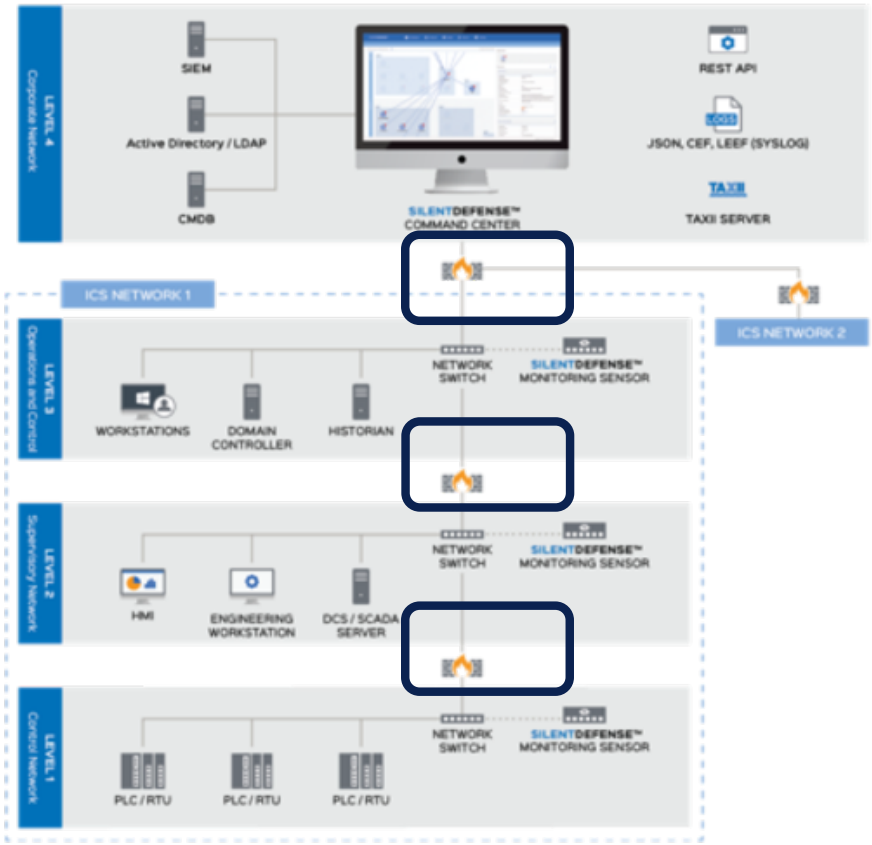
2016: 25 people, first (and only) funding round

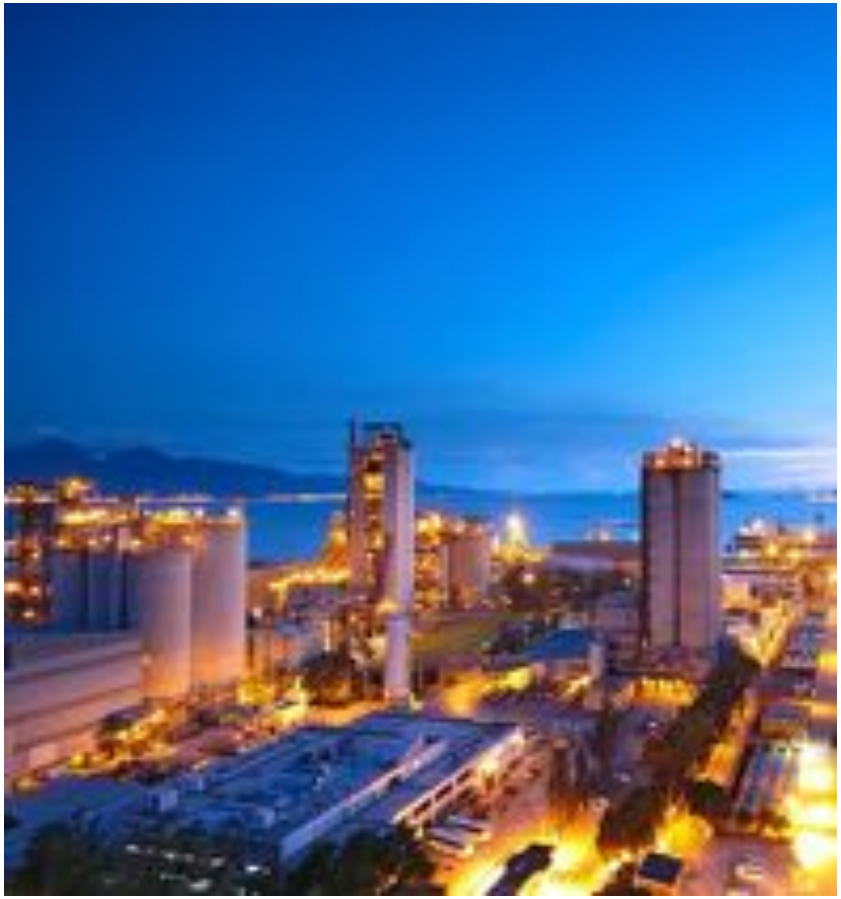
2017: 50 people at YEnd

11/2018: almost 100 people & EXIT

SecurityMatters in 2012

The product, eventually: Network Monitoring of Industrial Control Systems (ICS)





What are we proud of

- Pioneer of a new approach
  - other followed
  - (and in some cases we followed back)
- Throughout the years, the #1 company in the space
- 10 PhD graduates (4 “mine”)

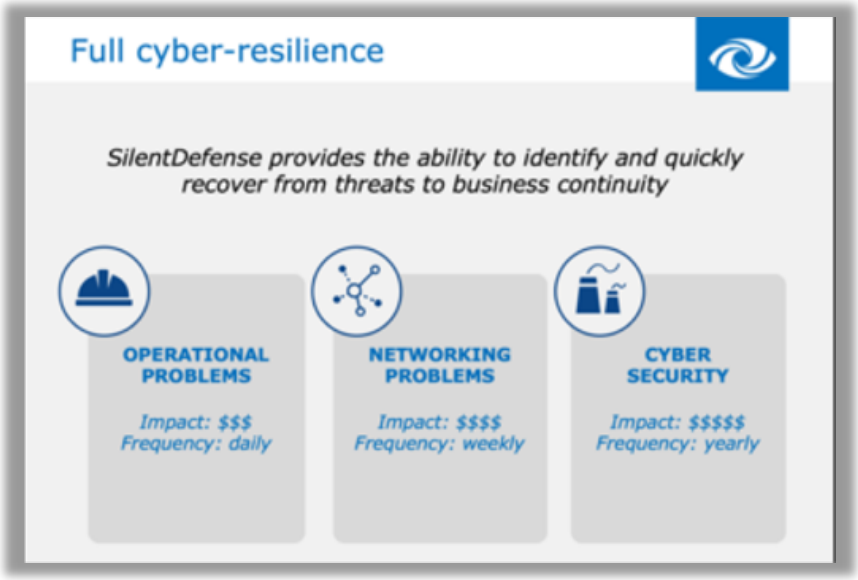
SecurityMatters, the failures

- Too many to mention

- **Pivoted** a few times
- You always need a plan-B
- And a plan C, a plan D etc.

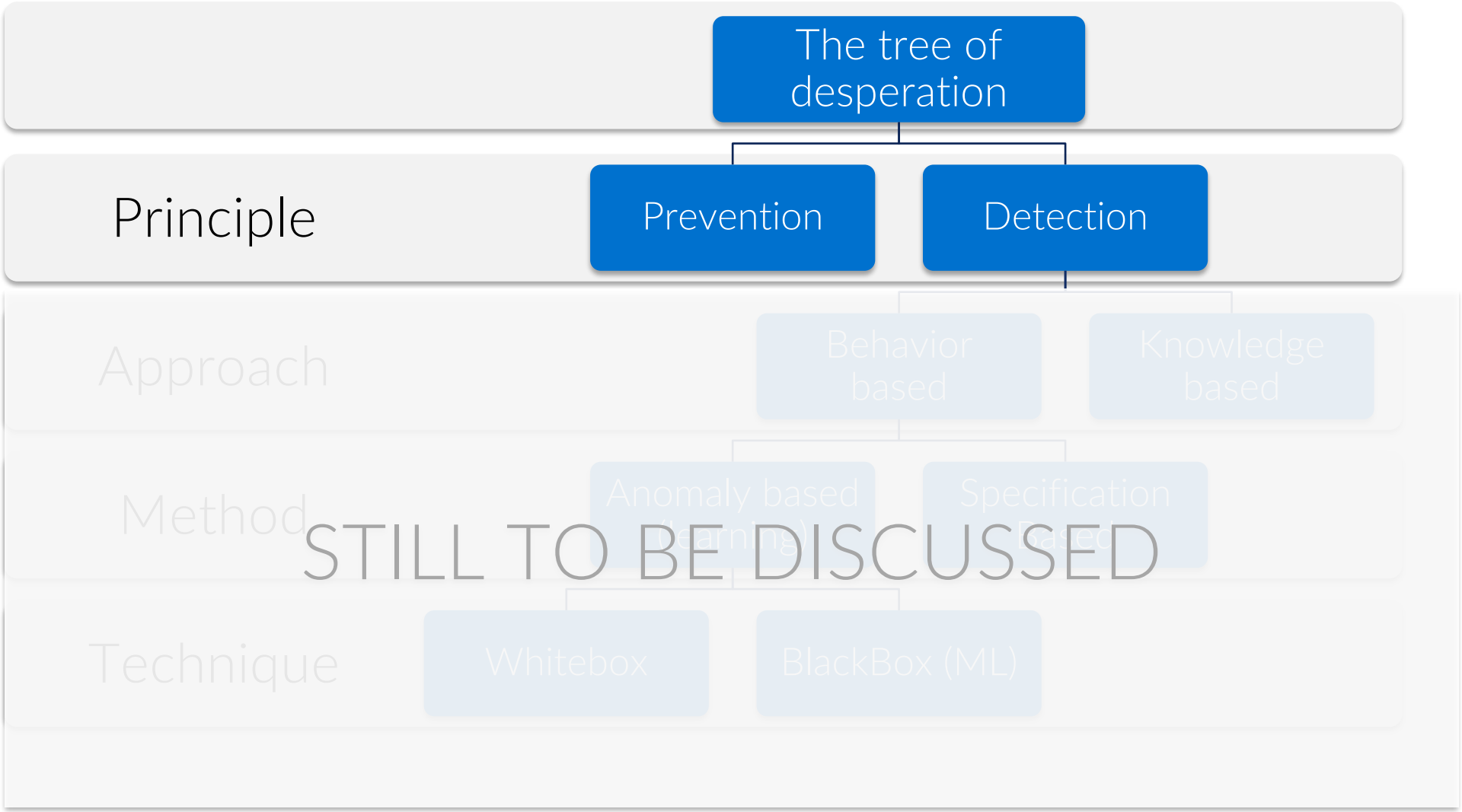
Key Technical Winning Elements (eventually…)

- Focus on ICS
- Focus on the Operational Problems
- No “Security” but “CyberResilience”
- No “Detection” but “Visibility”



LET’s TALK ABOUT DEFENCE

Two Ways of Dealing with Attacks



The Solution: Prevention?

- SW will never be 100% bug-free
- and even if it were 100% bug-free, it would be used in an insecure way
- and even if it were used in a secure way, something else will eventually spoil the system. There are too many connections
- And even then ….

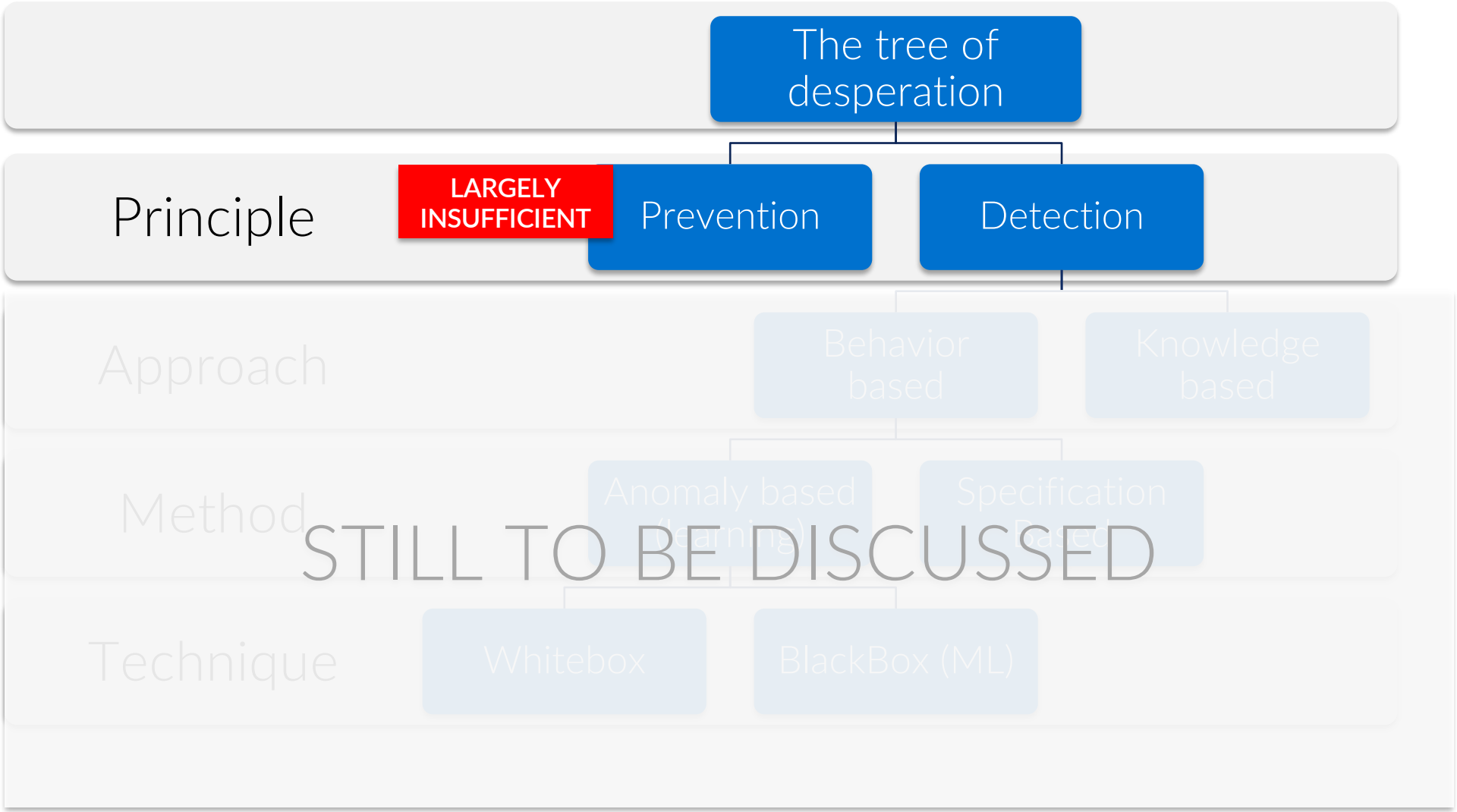
The Washington Post
Democracy Dies in Darkness

Innovations

How a fish tank helped hack a casino

By Alex Schiffer July 21

The possibilities (in my opinion…)



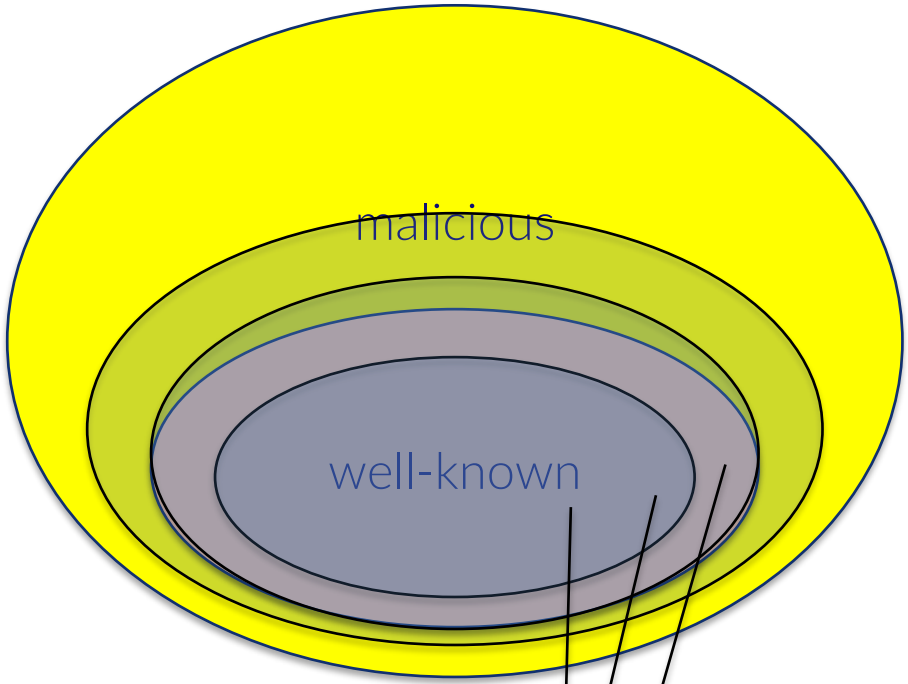
LET'S START DIGGING INTO IDSS

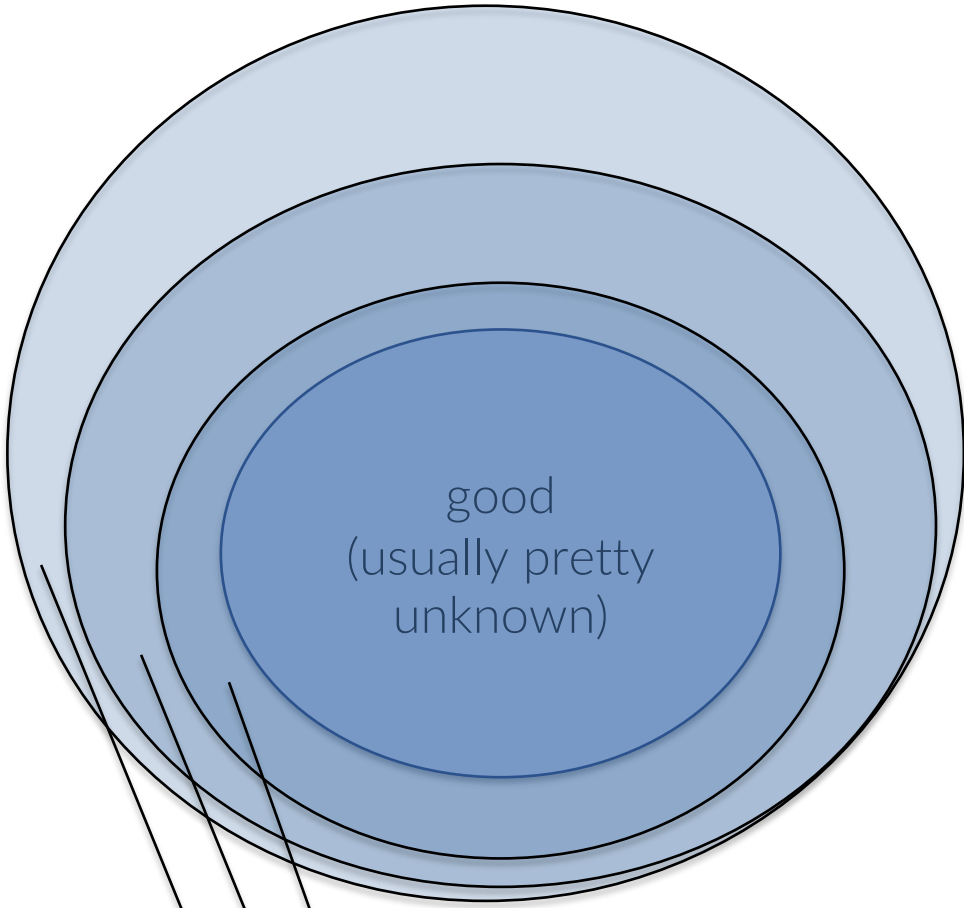
How can you detect an attack.

- **Knowledge-Based**
  - **Negative model** aka **blacklisting**
  - You recognize the attack
  - Anti-viruses, Blacklisting, Signatures, etc…

- **Behavior Based**
  - **Positive model**: you recognize the **normal behavior**
  - what is not normal, is an attack, or in any case it is **worth looking at**
  - e.g. firewalls, whitelisting systems,

In other words





very specific signatures

less specific rules, emulation

generic experimental stuff

- the size of circles is arbitrary
- these are just examples

very specific whitelisting

generic whitelisting (e.g. WA firewalls)

anomaly detection

Let's take care of knowledge-based systems

- **They detect a fraction of the attacks**.
  - Too bad, because they score very well on the other criteria
- For a lot of systems you don't have the knowledge
- … or it is not cost effective to process it
- Too easy to evade

They Named it — Einstein, But $6 Billion Firewall Fails to Detect 94% of Latest Threats

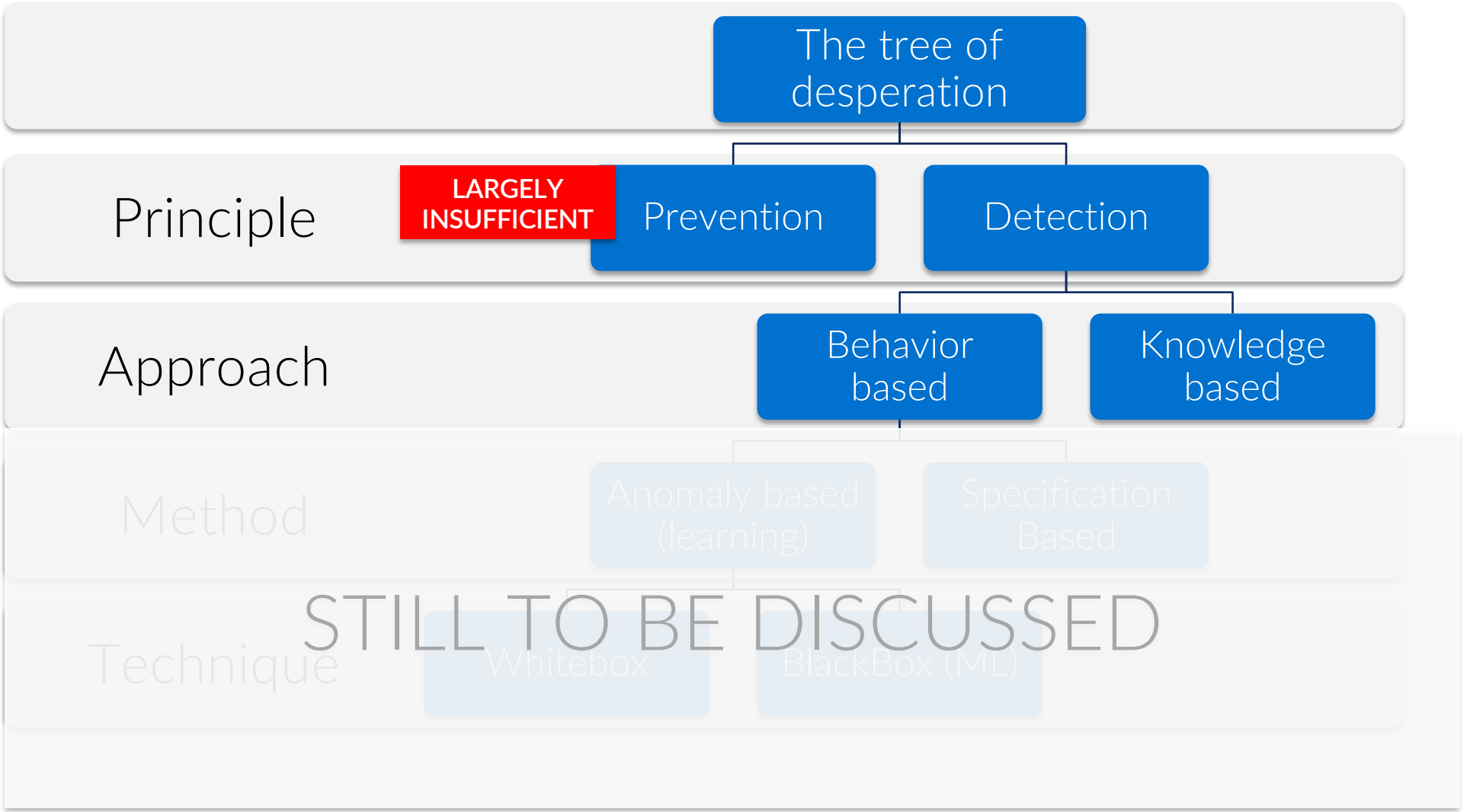
Tuesday, February 02, 2016 Swati Khandelwal

158 Like 14 Share 686 Tweet 259 Share 42 Share 1105

The US government's $6 Billion firewall is nothing but a big blunder.

Dubbed **EINSTEIN**, the nationwide firewall run by the US Department of Homeland Security (DHS) is not as smart as its name suggests.

So this is the situation…



So what is Behavior-based Intrusion Detection

- Exactly the area where ***"despite extensive academic research one finds a striking gap in terms of actual deployments of such systems"***
  - Robin Sommer, Vern Paxson: Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. S&P 2010

- [PROBLEM]:
  - The way academic IDSs are evaluated is unrealistic. [IMHO]
  - It is very difficult to evaluate IDS properly.

When do we have a GOOD IDS?

- Research papers look at only two parameters
  - Low **False Negatives** (high **detection rate)**: effectiveness
    - Also in presence of new attacks
  - Low **False Positives** rate. High FP => High Usage Costs

- IMHO
  - Regarding the detection rate, papers usually indicate 90%+, but 50% detection rate would be more than sufficient, if *it was for real attacks (attacks are multistep anyhow)*
  - False positive rate is very important and my rule of thumb is that it should be < 0,01% to be viable.
  - BUT : these parameters are not enough to evaluate an IDS

When evaluating an IDS we should also look at:

- **Actionability**
  - how much information does the IDS give the user to prepare the response? No information => Very High Usage Costs
- **Adaptability**.
  - Most IT systems change continuously (even SCADA systems, for that matter). The IDS operational costs are heavily affected by the cost of adapting it to the system changes.
- **Scalability**.
  - How much does it cost to install and operate the IDS when deployed on 2, 200 or 2000 networks?
- IMHO:
  - lack on these fronts are the reason why "despite extensive academic research one finds a striking gap in terms of actual deployments of such systems"
  - Of course these parameters are difficult to evaluate in an academic setting
  - Did I mention it is a "horrible" research area?

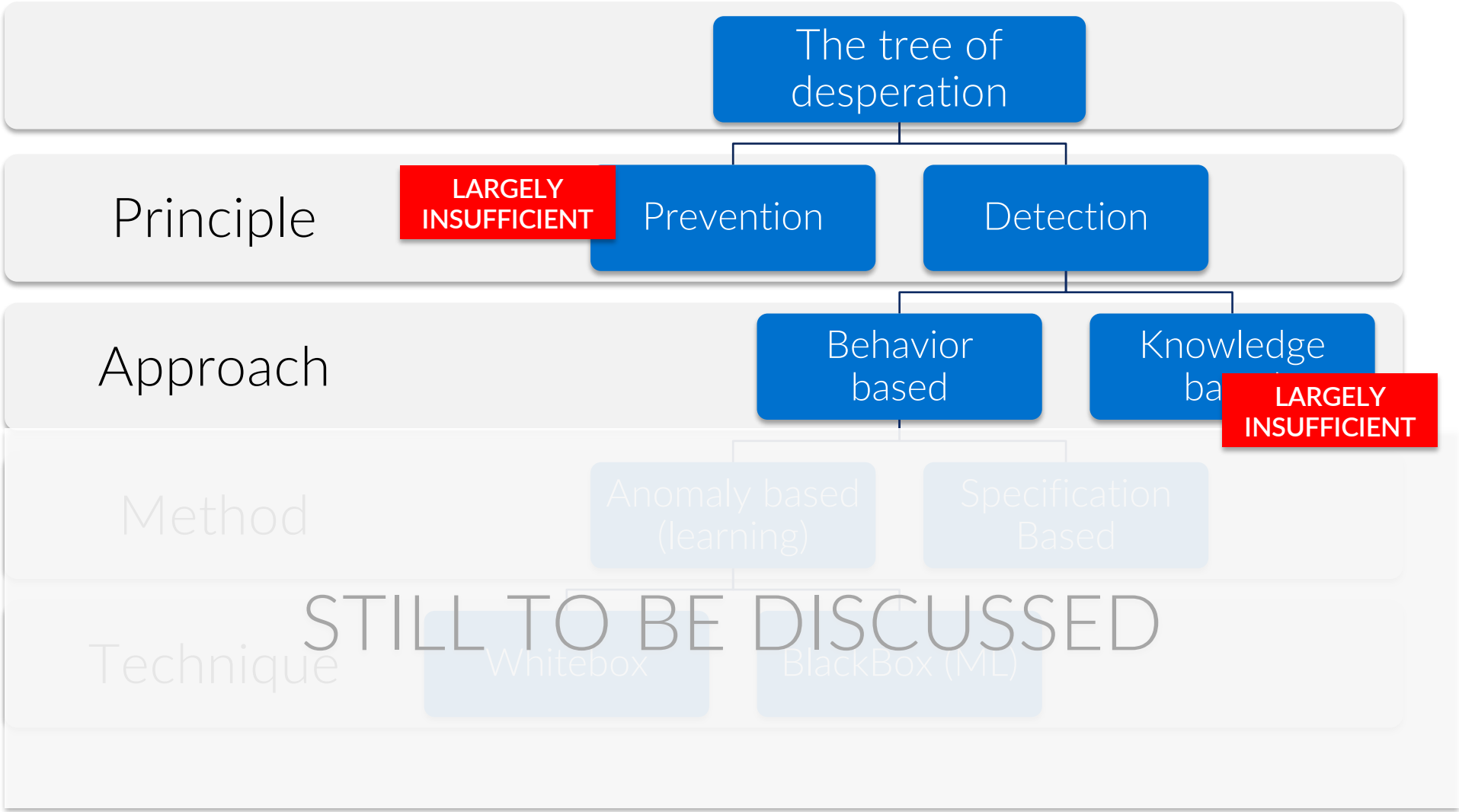
It's all 'bout the money….

- If you think this is silly, think about the amount of effort *monitoring* requires

- There are simply not enough people to monitor our infrastructure, (with anything else than a signature-based system), let alone time to teach them how to do it and money to pay them

- Therefore:
  - False Positives are a problem, False Negatives are much less so
  - Actionability, Adaptability, Scalability are key, because they save time and money

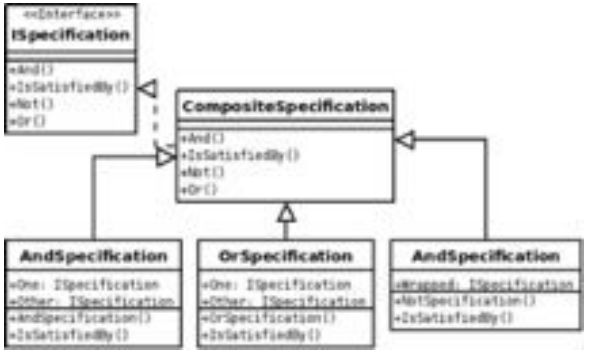
The possibilities (in my opinion…)



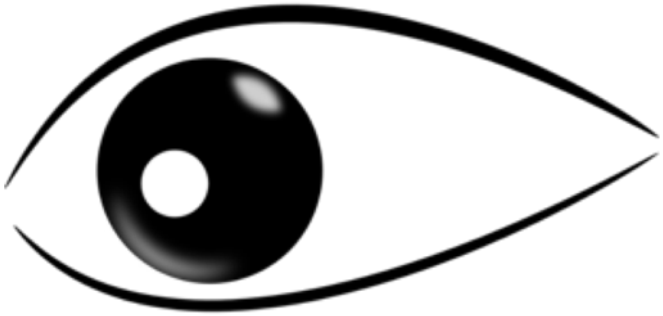
So we are left with behavior-based systems

- Where do we get the knowledge about the system?

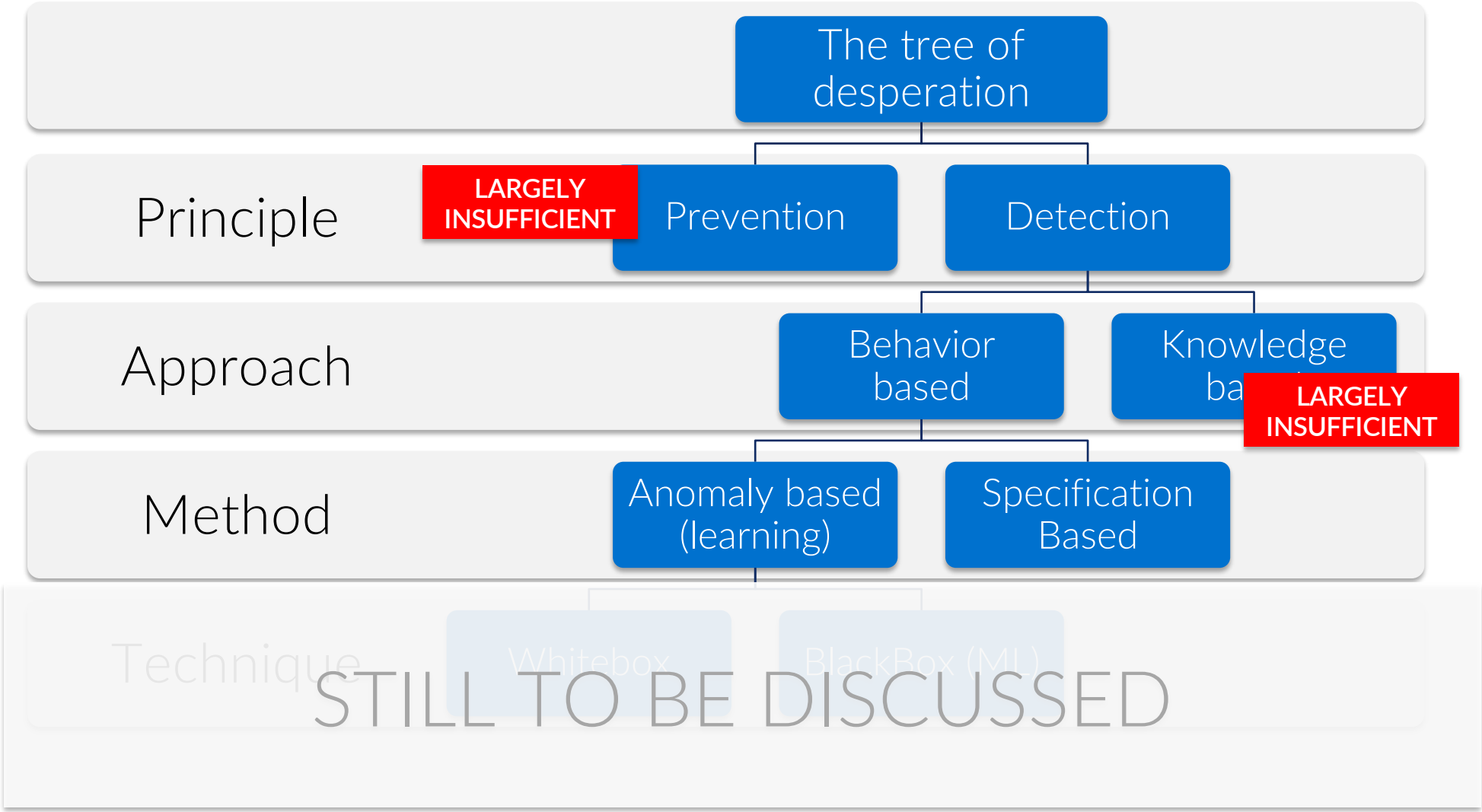
- From a specification,
  - (specification-based systems)



- We learn it automatically
  - (“anomaly-based systems”)



So we are in this situation

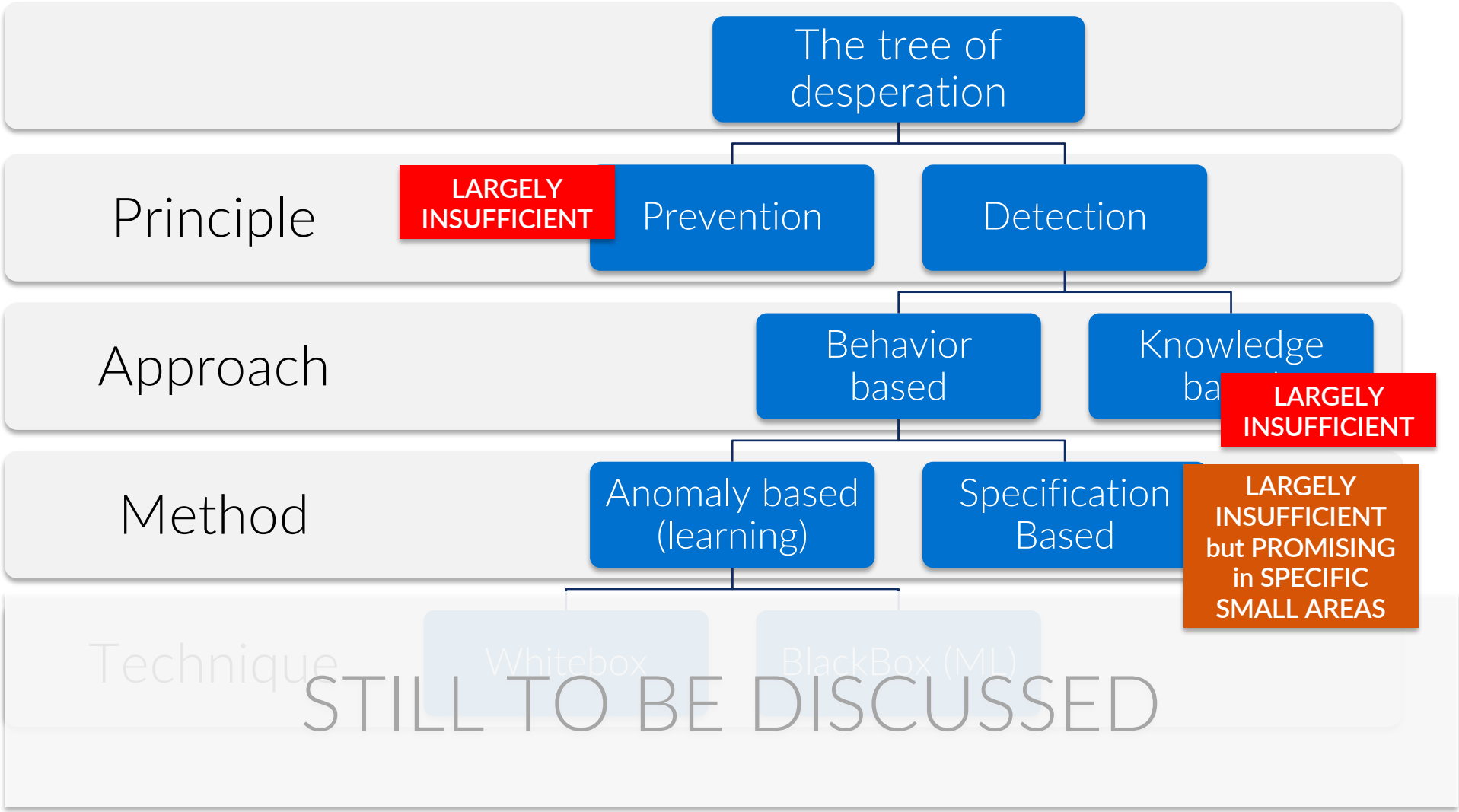


Specification-based systems are … challenging

- Two crucial features they do not satisfy “by definition”
  - **Adaptability**. Most IT systems change continuously (even SCADA systems, for that matter)
  - **Scalability**. How much does it cost to install and operate the IDS when deployed on 2, 200 or 2000 networks

- In 2017 I was more optimistic (I wrote “I love the principle of specification-based systems, I think it will become increasingly popular, I believe it will be applicable and applied only to specific subparts of a system of systems (think of IoT….))
- but now I am more skeptical: systems change too fast and too often (think of patches, updates etc). Even physical systems are increasingly unpredictable.
- But: ”light specifications” can help a lot

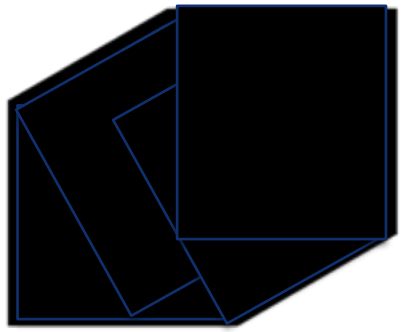
The possibilities (in my opinion…)



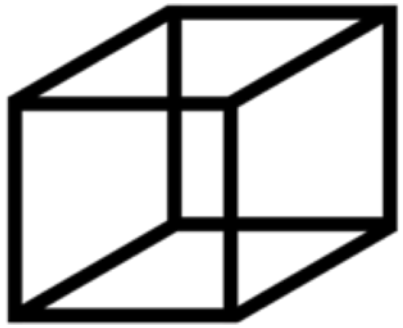
And now we are left with anomaly-based systems

- Another splitting, in two flavors:

  - **BlackBox**, using machine learning approaches, like neural networks.
    - The semantics used by the detection system is "unrelated" to the semantics of the target system



  - **WhiteBox**,: the semantics used by the detection system is "an abstraction" of the one one of the target
    - we try to *explain* the semantics of the target system
    - Based on e.g. understanding the communication protocol, extracting command and setpoints and whitelisting them.

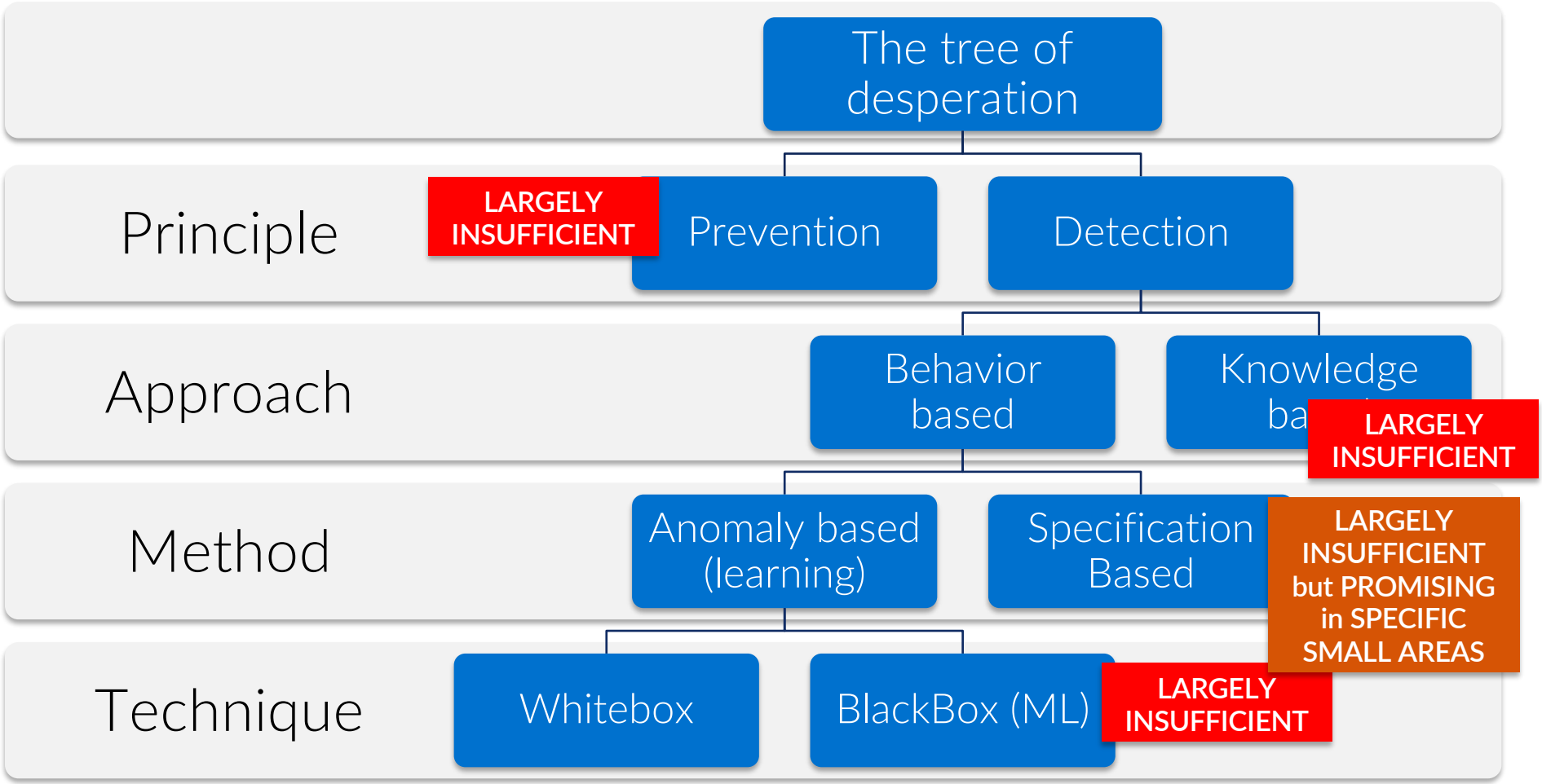


BlackBox Systems are not the solution

- **Personal Opinion 1**
- **I believe that blackbox anomaly-based intrusion detection systems are of very limited use for security.**
  - Actionability is the main problem
  - But also FPs and Adaptability

- Sommer and Paxson (S&P 2010)
  - "we deem it crucial for any effective deployment to acquire deep, semantic insight … rather than treating the system as a black box as unfortunately often seen. "
  - "the better we understand the semantics of the detection process, the more operationally relevant the system will be."
  - [blackbox] anomaly detection systems face a key challenge of transferring their results into *actionable* reports …. In many studies, we observe a lack of this crucial final step.

The possibilities (in my opinion…)



This should better be working

- It works! But: on specific systems
  - even on some large-scale systems.
  - good usability results on SCADA/ICS
  - a solution for all problems? No
  - By definition in anomaly detection: there is not a one-size fits all.

- **Personal Opinion 2**
- "Useful" anomaly-based intrusion detection **is not quite about intrusion detection; it is about being able to understand what happens in the target system** and being able to monitor its integrity.

Understanding is key

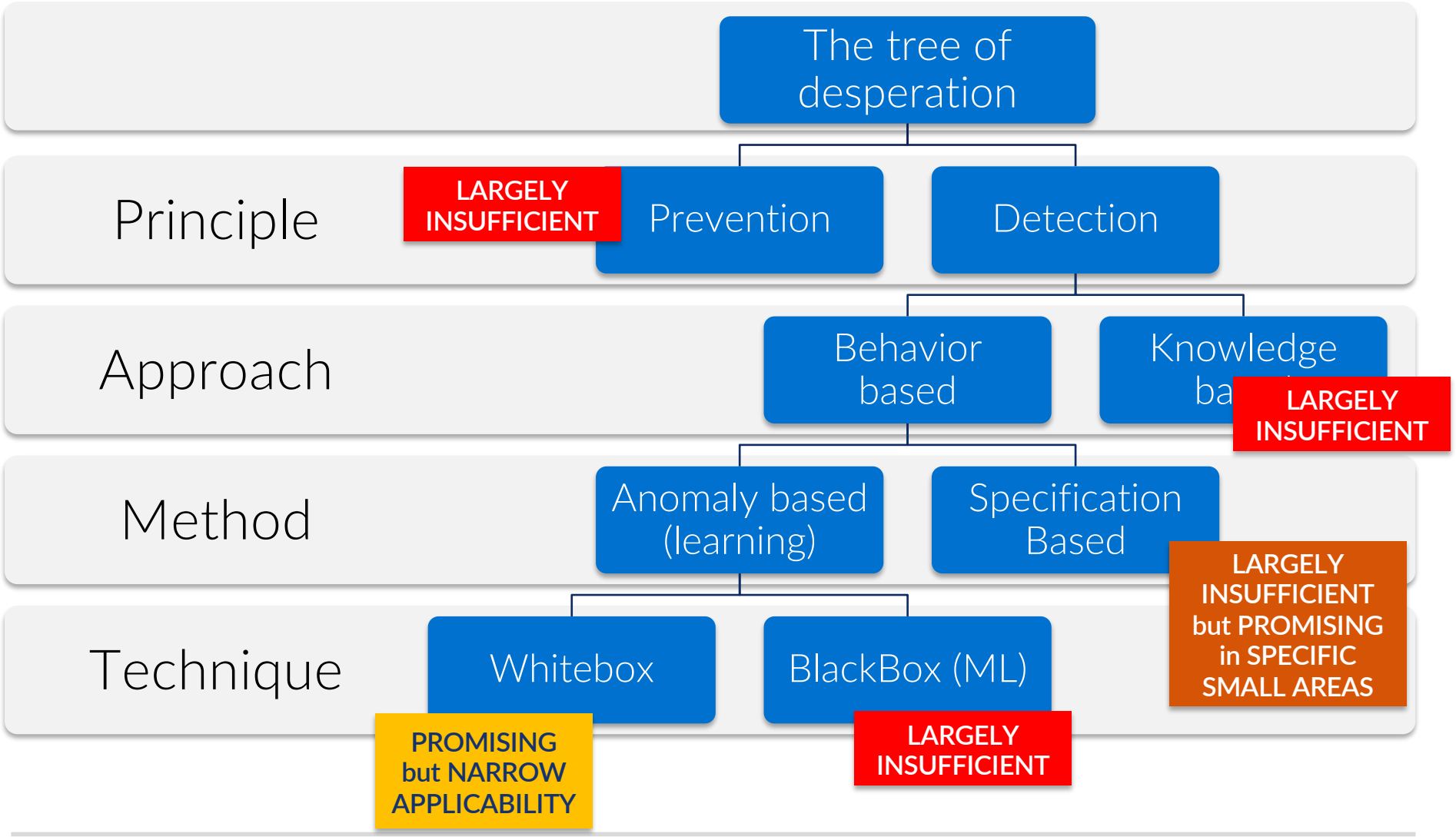
- If you understand what happens, then
  - You have a chance of understanding how the system should evolve (**adaptability**)
  - You are able to give a context to your alerts ("this is what was happening (context), and suddenly we see a message" (**actionability**)
  - (with a bit of luck) You can replicate the reasoning across similar systems (**scalability**)

Where Whitebox Anomaly Detection Fails

- *most IT systems are simply not understandable*
  - Too complex, too dynamic too much of a mess.
  - Try to do anomaly detection on the first picture…

- **Personal Opinion 3**
- **There cannot be a one-size-fits-all anomaly-based network intrusion detection system** that works equally well on all domains.

WE GOT STUCK


The tree of desperation
Principle
LARGELY INSUFFICIENT
Prevention
Detection
Approach
Behavior based
Knowledge ba
LARGELY INSUFFICIENT
Method
Anomaly based (learning)
Specification Based
LARGELY INSUFFICIENT but PROMISING in SPECIFIC SMALL AREAS
Technique
Whitebox
BlackBox (ML)
PROMISING but NARROW APPLICABILITY
LARGELY INSUFFICIENT

I believe that today the single most important reason why attacks are so difficult to counter is that

present systems are so hard to monitor

I believe the only practical way towards making more secure systems goes through

Designin software more “supervisable”, that is, less hard to monitor