How To Think Like a Security Analyst of Today

Raymond Carney

Consultant Technologist,
RSA NetWitness Product Management

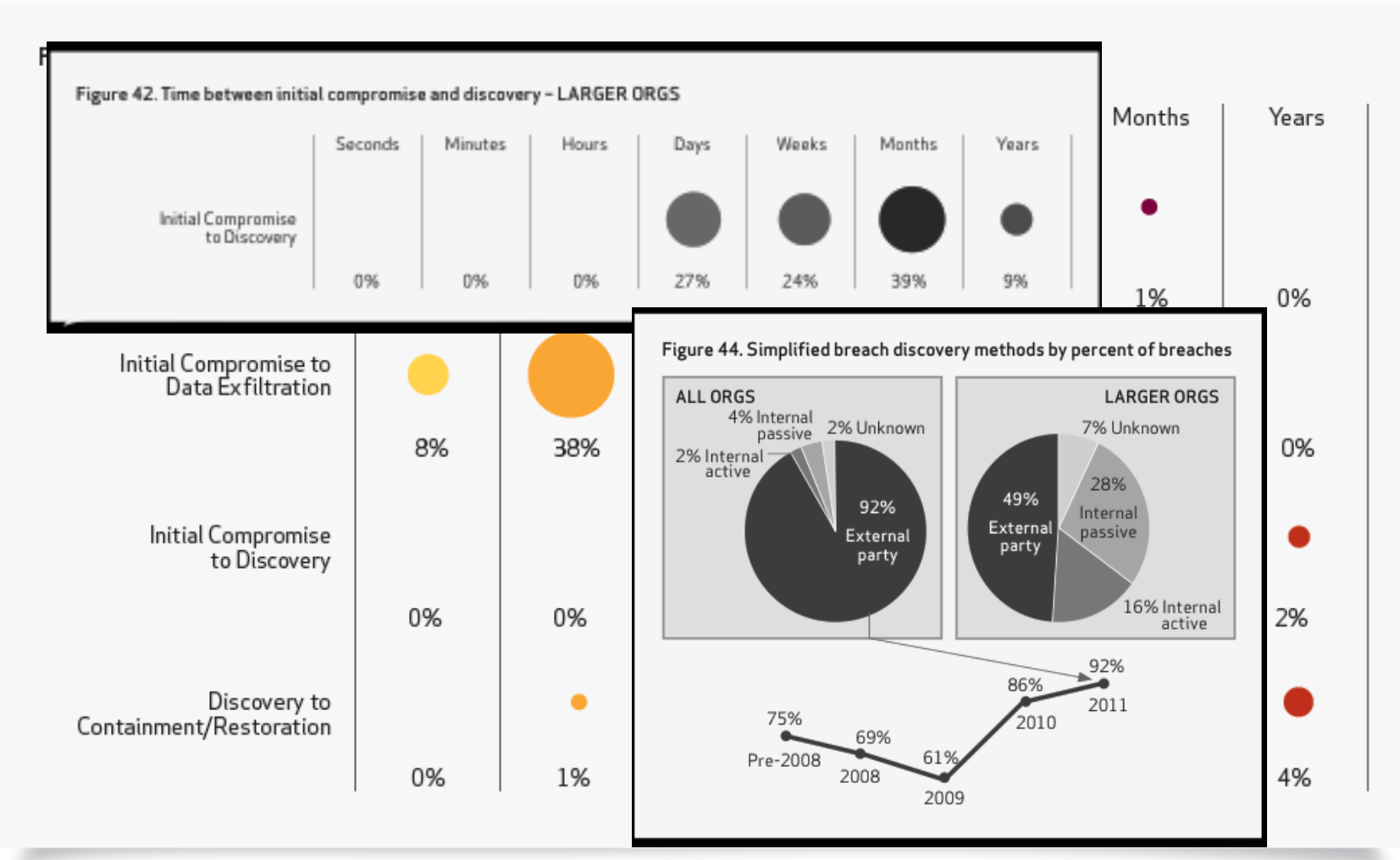
Today's Security Market Is Broken

- Traditional approaches to today's advanced adversaries and threats is not enough
- Failed solutions due to an incomplete view of threat actors and vectors
- **99%** of breaches led to compromise within "days" or less with **85%** leading to data exfiltration in the same time*
- **85%** of breaches took "weeks" or more to discover*

*Source: Verizon 2012 Data Breach Investigations Report

Want Proof?

Attacks lead to compromise and exfiltration within minutes, discovery takes months



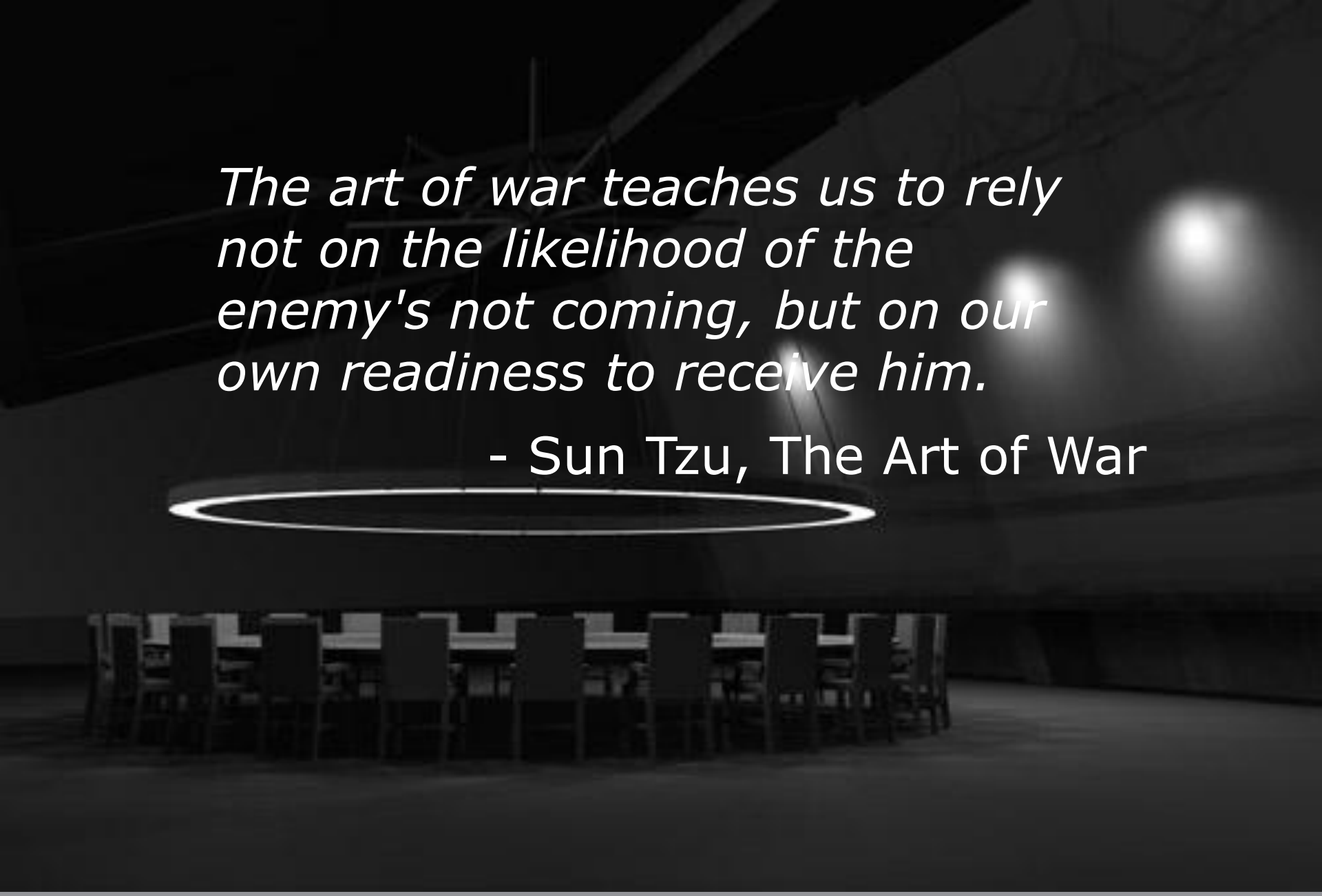
** Source: 2012 Verizon DBI*

There's something here that doesn't make sense…

Let's go poke it with a stick.

The Hard Truth

- Most organizations don't know enough about contemporary threats or their own security posture to defend themselves adequately against the rising tide of cyber attacks.
- Successful defense against these threats requires evolving past conventional approaches to information security
- It's not about writing packets to disk, or finding a particular piece of malware… it's all about the *analytics*.



Critical questions that we will address

- What are the basic requirements for building an intelligence capability?
- What are some of the best sources of data?
- How can you design a process that will consistently produce actionable intelligence and the right defensive strategies?
- How can you implement automation to help create efficiencies in handling large volumes of data?

Q: Why are Information Security teams losing the fight against today's threats?

A: Lack of sufficient Actionable Intelligence

- Intelligence gathering and analysis are increasingly essential capabilities for a successful information security program.
- Most information security organizations have not been built with this objective in mind.
- Evidence indicates that, by and large, the "Bad Guys" have developed better intelligence capabilities than the "Good Guys".
- *How do we get there?*

A Roadmap for Intelligence-driven Security Program

1. Start with the Basics
   - *Inventory strategic assets, strengthen incident-response processes and perform comprehensive risk assessments.*
2. Make the Case
   - *Communicate the benefits of an intelligence-driven security program to executive management and key stakeholders. Identifying "quick wins" to prove value out of the gate is essential for gaining broad organizational support, including funding.*
3. Find the Right People
   - *Look for professionals who can blend technical security acumen with analytical thinking and relationship-building skills.*
4. Build Sources
   - *Determine what data from external or internal sources would help detect, predict or lessen the chances for a targeted attack; evaluate sources on an ongoing basis.*
5. Define a Process
   - *Codify a standardized methodology to produce actionable intelligence, ensure an appropriate and timely response and develop attack countermeasures.*
6. Implement Automation
   - *Find opportunities to automate the analysis and management of large volumes of data from multiple sources.*

Let's start with some fairly basic questions...

- If you don't know the threat, how do you know what to protect?
- If you don't know what to protect, how do you know you're protecting it?
- If you're not protecting it…

The Adversary Wins!

"One of the biggest problems in the world of intelligence is that you quickly drown in data. You get masses of data, but you have to be able to derive knowledge from it, make it relevant and actionable – that takes good tools and better still excellent analysts."

Professor Paul Dorey,

Founder and Director, CSO Confidential and

Former Chief Information Security Officer, BP

Actionable Intelligence is knowledge that enables an organization to make informed risk decisions and take action.

What is Analysis?

What is Analysis?

1. Analysis is a process of inspecting, cleaning, transforming, and modeling data with the goal of highlighting useful information, suggesting conclusions, and supporting decision making.
2. Analysis is the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context (Warner, 2002)

- *Simplified*: analysis is a way of reducing the ambiguity of highly ambiguous situations

Role of the Analyst

- Simple answer: Provide decision support
  - The purpose of intelligence analysis is to reveal to a specific decision maker the underlying significance of selected target information.

A little more detail…

- Provide a leading role in development of intelligence work plans for portfolios addressing specific security threats.
- Utilize and develop the use of a broad range of intelligence-related databases, tools and systems to conduct complex analysis
- Develop subject matter expertise on specific as well as general security threats.
- Conduct, and guide teams in, complex research and analysis on current and emerging trends in relation to specific security threats.
- Support intelligence operations by providing guidance and quality assurance in the compilation of intelligence products which address recognized security threats.
- Provide timely security threat intelligence to inform and shape the planning and conduct of surveillance and response operations in support of business objectives.

12 Analyst Hats..

- Reporter
- Detective
- Consultant
- Diagnostician
- Investigator
- Organizer
- Puzzle Solver
- Evaluator
- Simplifier
- Forward Observer
- Artist
- Sculptor

Let's make it a Baker's Dozen…

- Epistemologist
  - epistemology |iˌpistəˈmäləjē|
    - The theory of knowledge, esp. with regard to its methods, validity, and scope.
    - Epistemology is the investigation of what distinguishes justified belief from opinion.

- *Become truly neutral*
- *Accept that we are all subject to cognitive biases*
- *Know and understand the differences in A Priori and A Posteriori knowledge*
- *Use Structured Analytic Techniques to avoid pitfalls*

"A man's got to know his limitations."

Harry Callahan

Are We There Yet?

"To study the abnormal is the best way of understanding the normal."

William James

American psychologist and philosopher

- *The inverse holds true as well, and is a central tenet to achieving our goals*

Understanding Intelligence

- Data
- Information
- Knowledge
- Intelligence
- Action

- Raw data needs to be reviewed, analyzed, and put into context in order to develop intelligence, which can then be used to make risk decisions.

Understanding Intelligence

- Data *(Capture)*
- Information *(Assemble)*
- Knowledge *(Parse)*
- Intelligence *(Index & Report)*
- Action *(Act on Guidance)*

- Raw data needs to be reviewed, analyzed, and put into context in order to develop intelligence, which can then be used to make risk decisions.

Digression: Network Forensics

What is Network Forensics?

- This ***was*** my favorite definition…

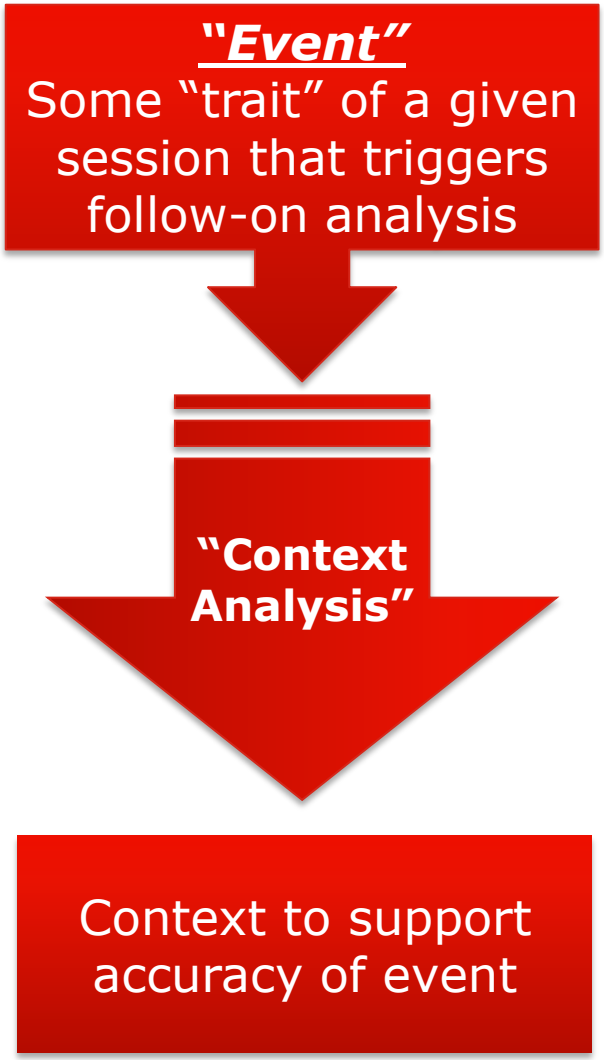
"Network forensics is the process of capturing information that moves over a network and trying to make sense of it in some kind of forensics capacity."

Network forensics in practice

- Traditional
  - Pcap / wireshark
  - IDS
  - IPS
  - Even products like FireEye…

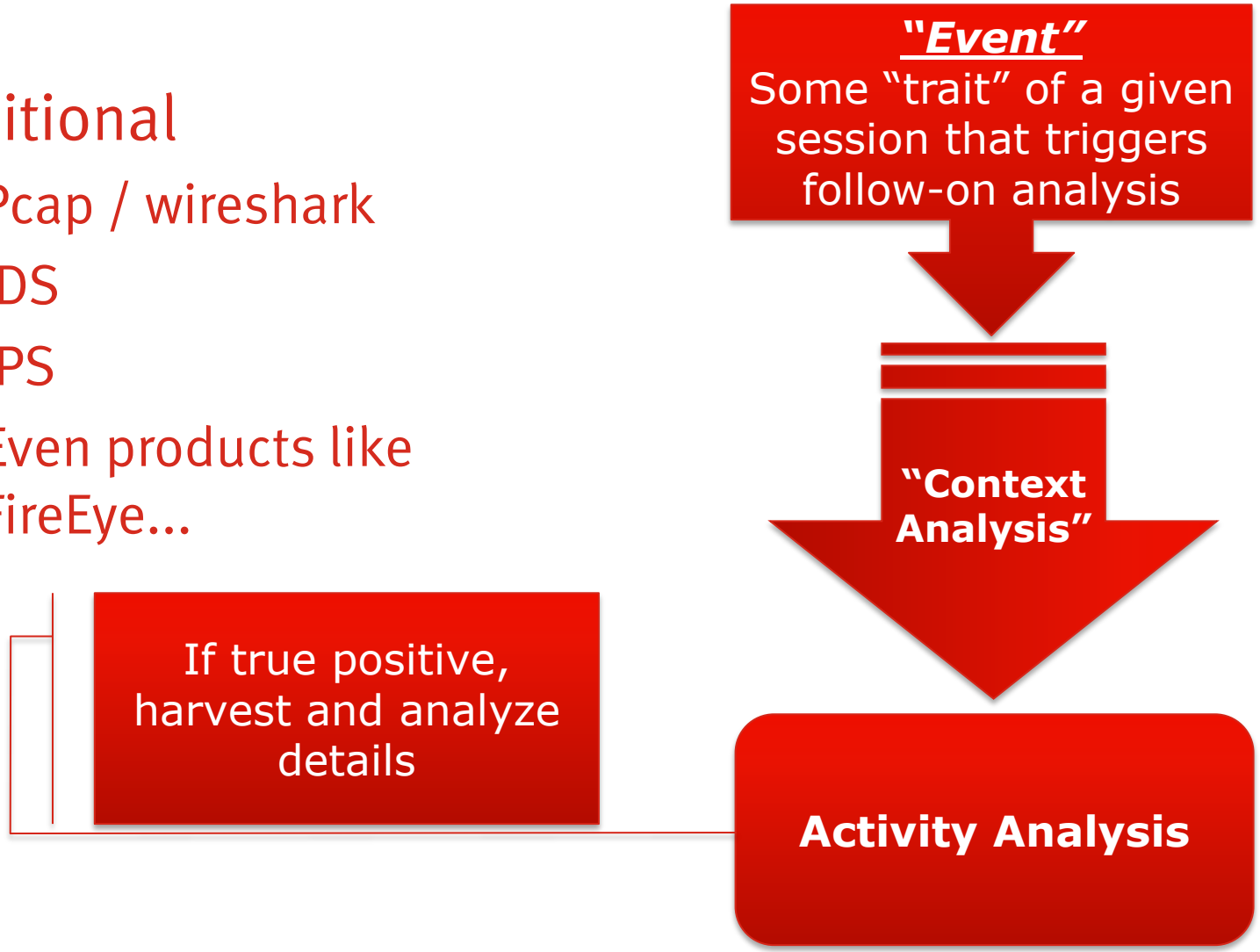
Network forensics in practice

- Traditional
  - Pcap / wireshark
  - IDS
  - IPS
  - Even products like FireEye…



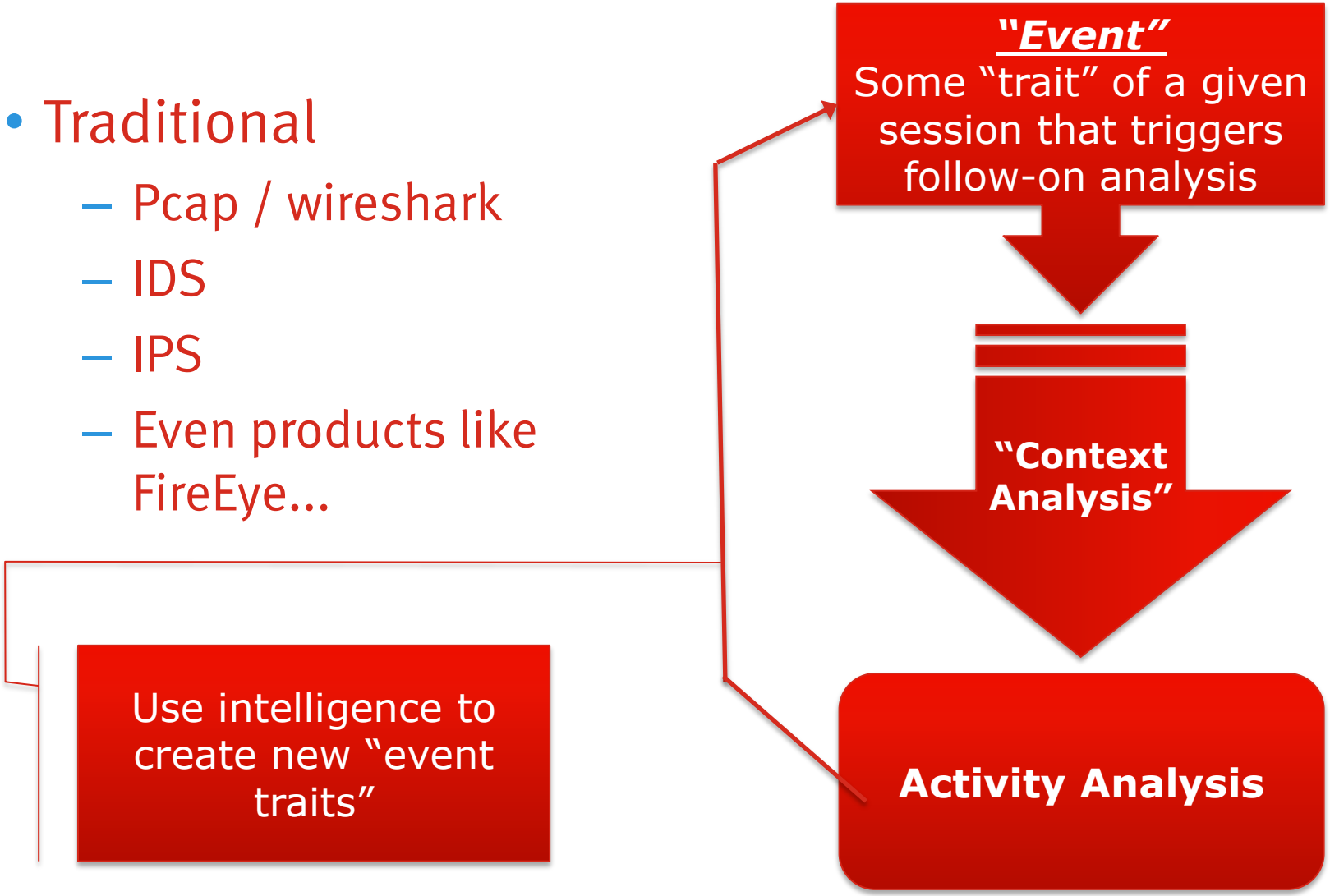
Network forensics in practice

- Traditional
  - Pcap / wireshark
  - IDS
  - IPS
  - Even products like FireEye…



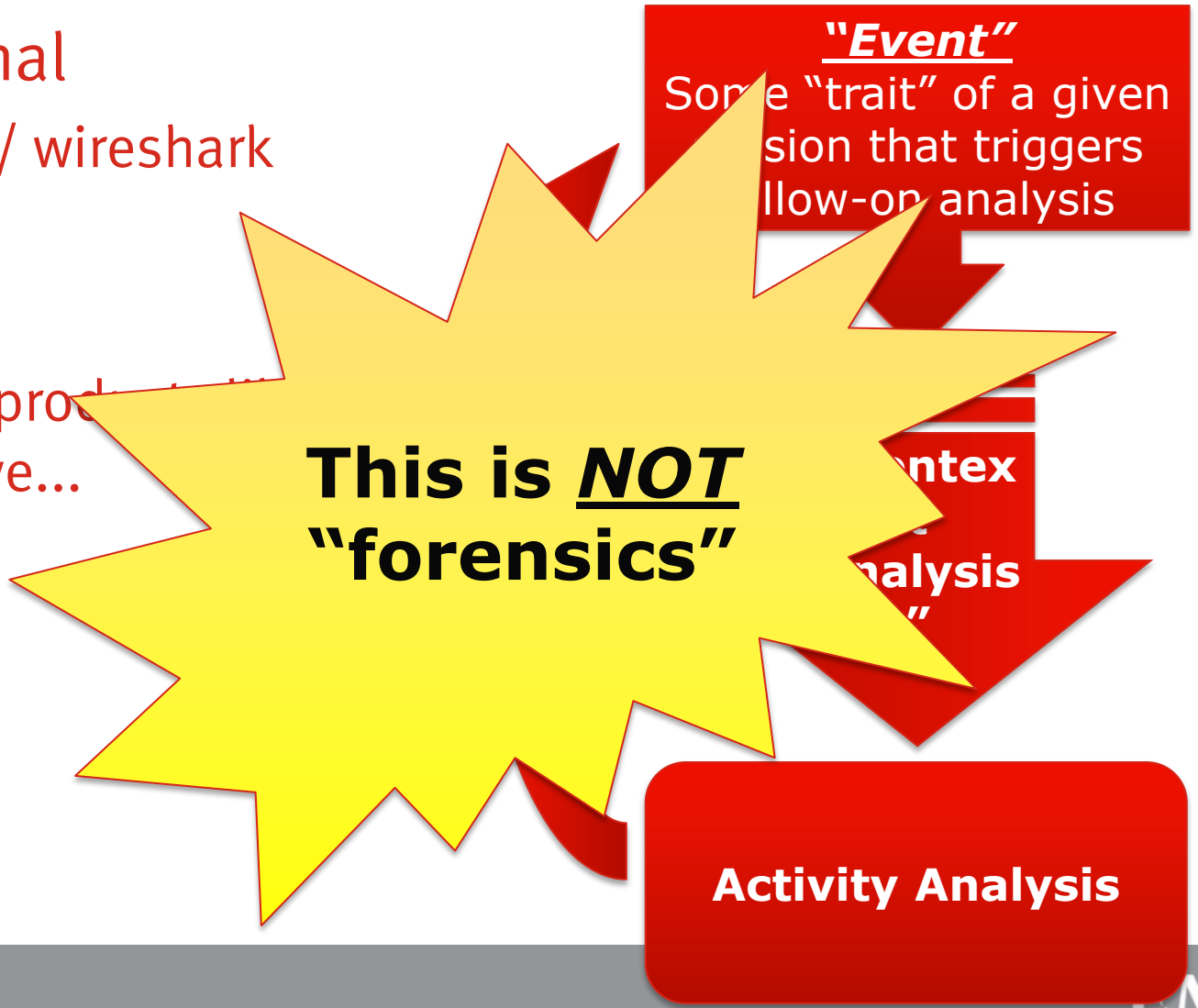
Network forensics in practice

- Traditional
  - Pcap / wireshark
  - IDS
  - IPS
  - Even products like FireEye…



Network forensics in practice

- Traditional
  - Pcap / wireshark
  - IDS
  - IPS
  - Even prod… FireEye…



Thinking that is forensics is why the Infosec industry is so bad at finding compromises

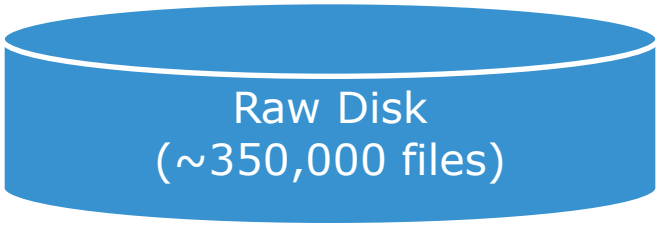
- But, before we dissect the reasons why, let's look at real forensics, as performed on the host...

Analogy: Host-Based Forensics

- Find malware

Analogy: Host-Based Forensics

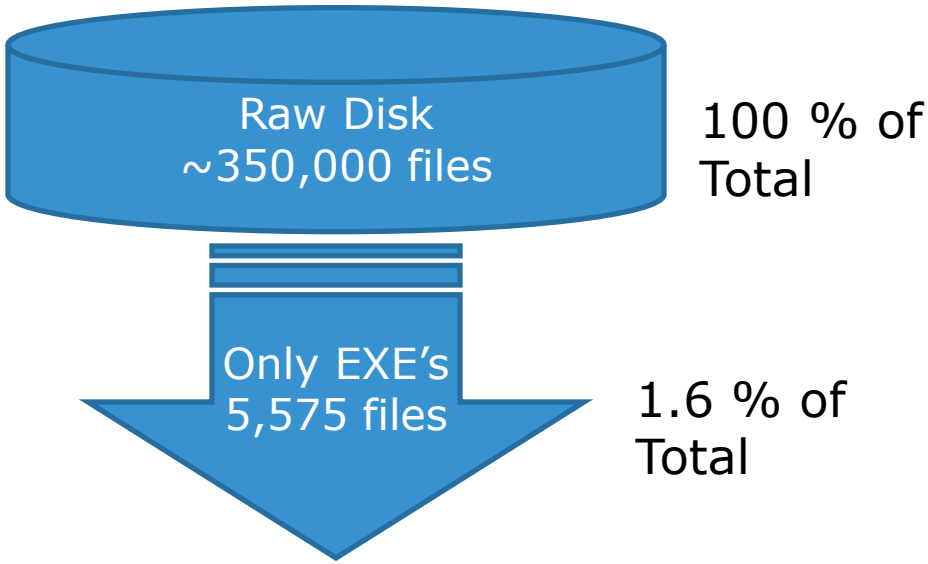
- Find malware



100% of Total

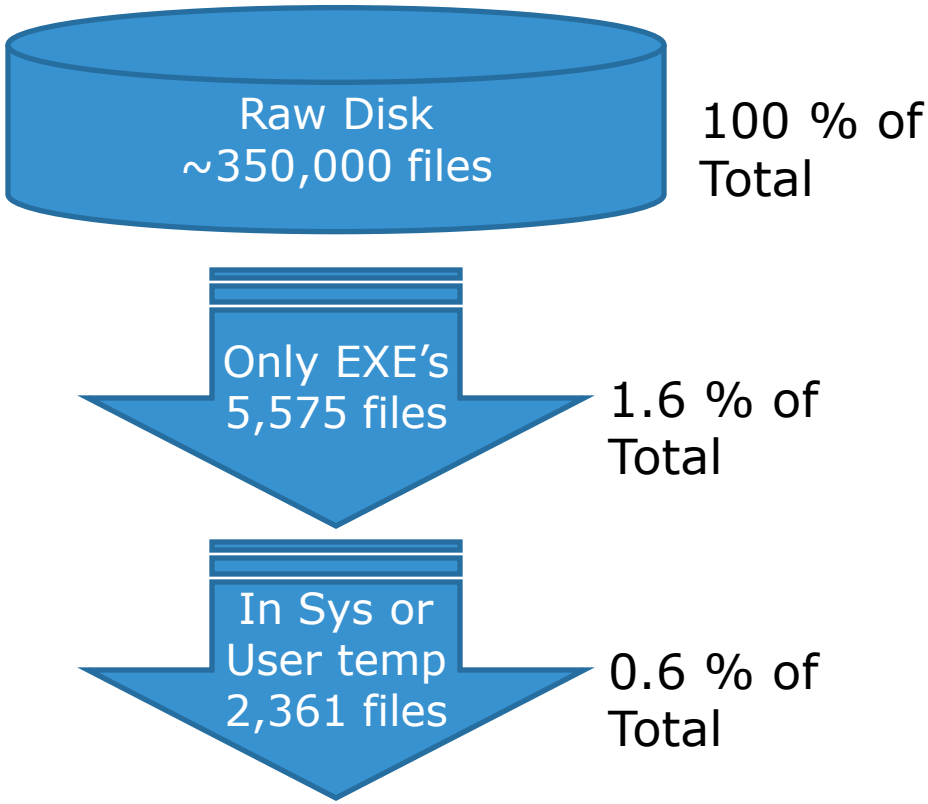
Analogy: Host-Based Forensics

- Find malware



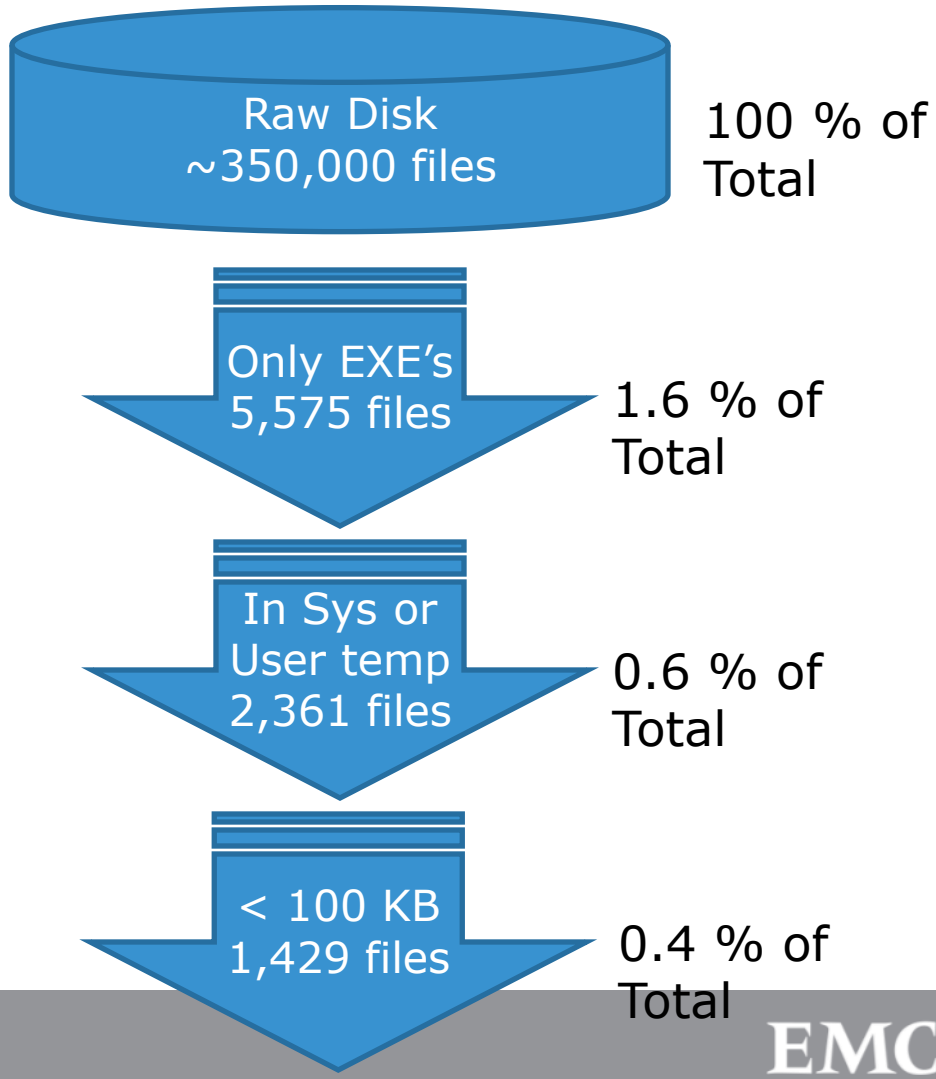
Analogy: Host-Based Forensics

- Find malware



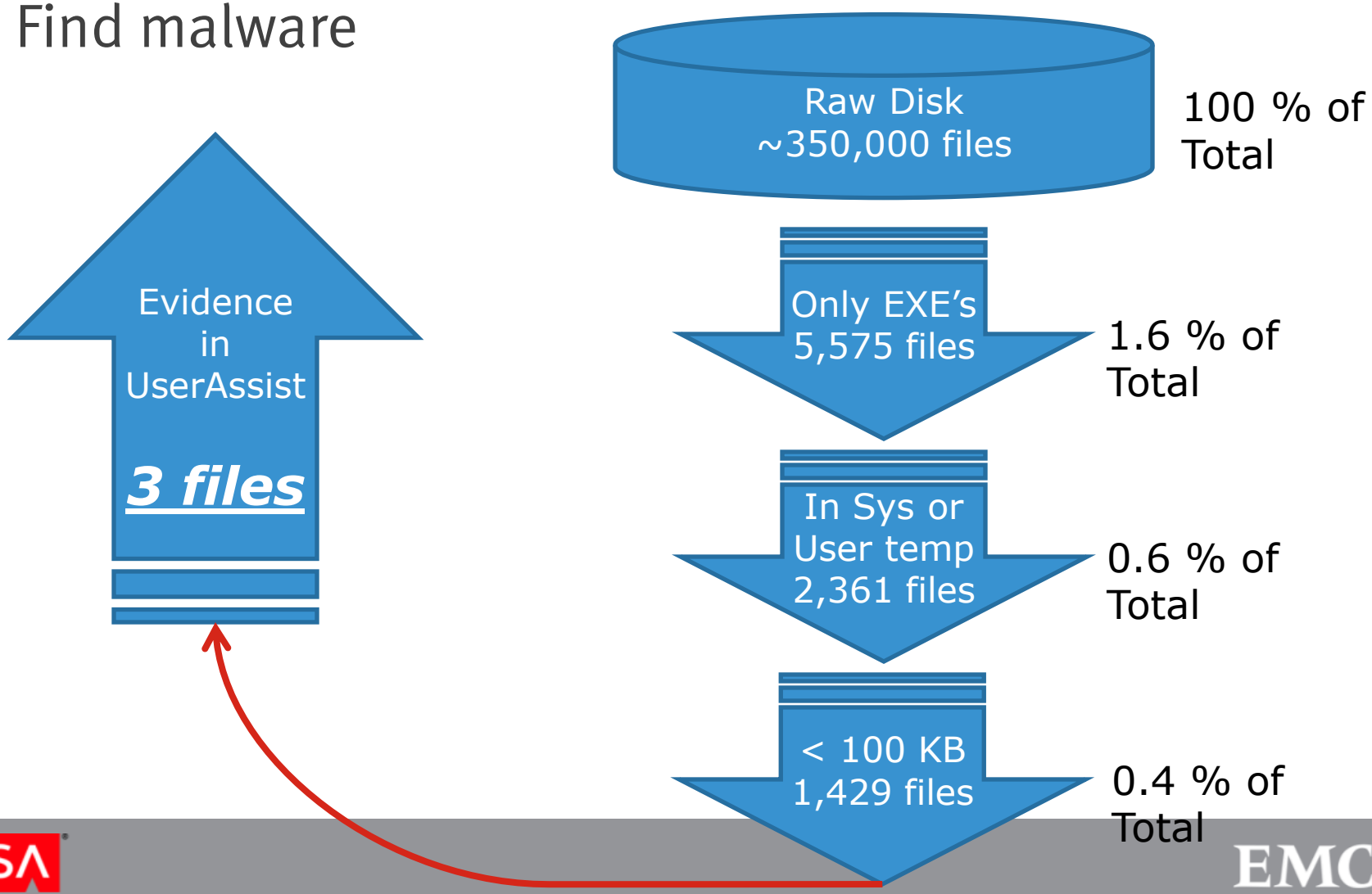
Analogy: Host-Based Forensics

- Find malware



Analogy: Host-Based Forensics

- Find malware



What just happened there???

We found malware…

…by NOT looking for malware!!!

Example: Good network forensics

- Find Compromises

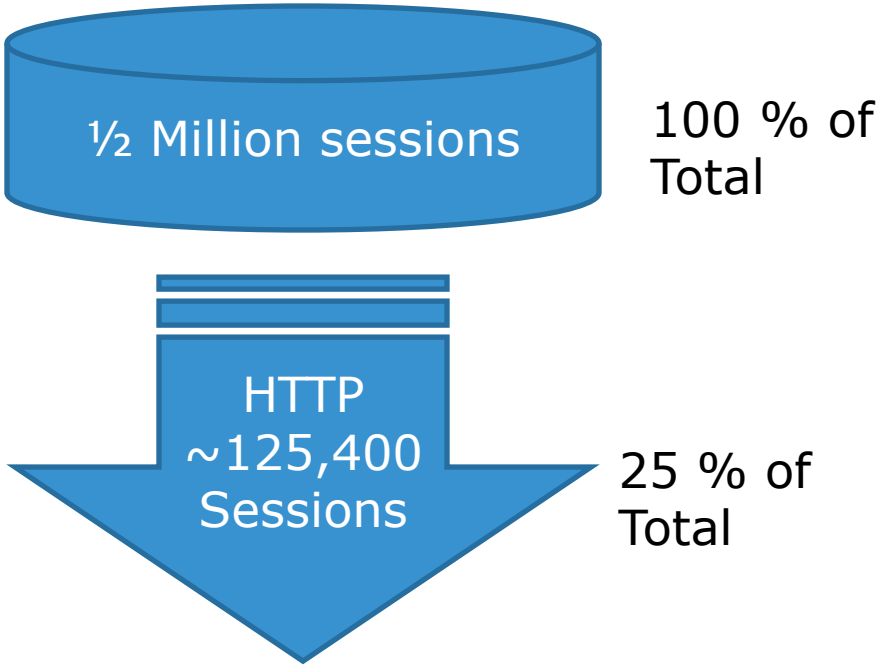
Example: Good network forensics

- Find Compromises

100 % of Total

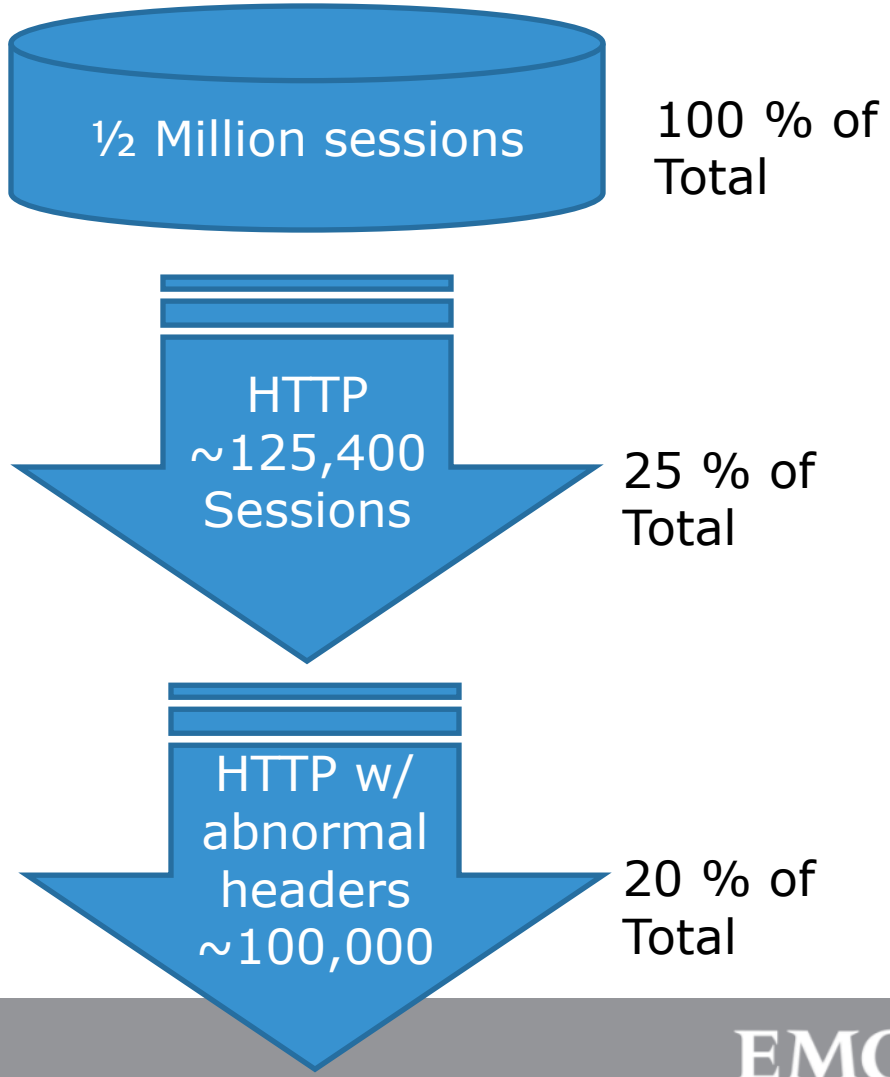
Example: Good network forensics

- Find Compromises



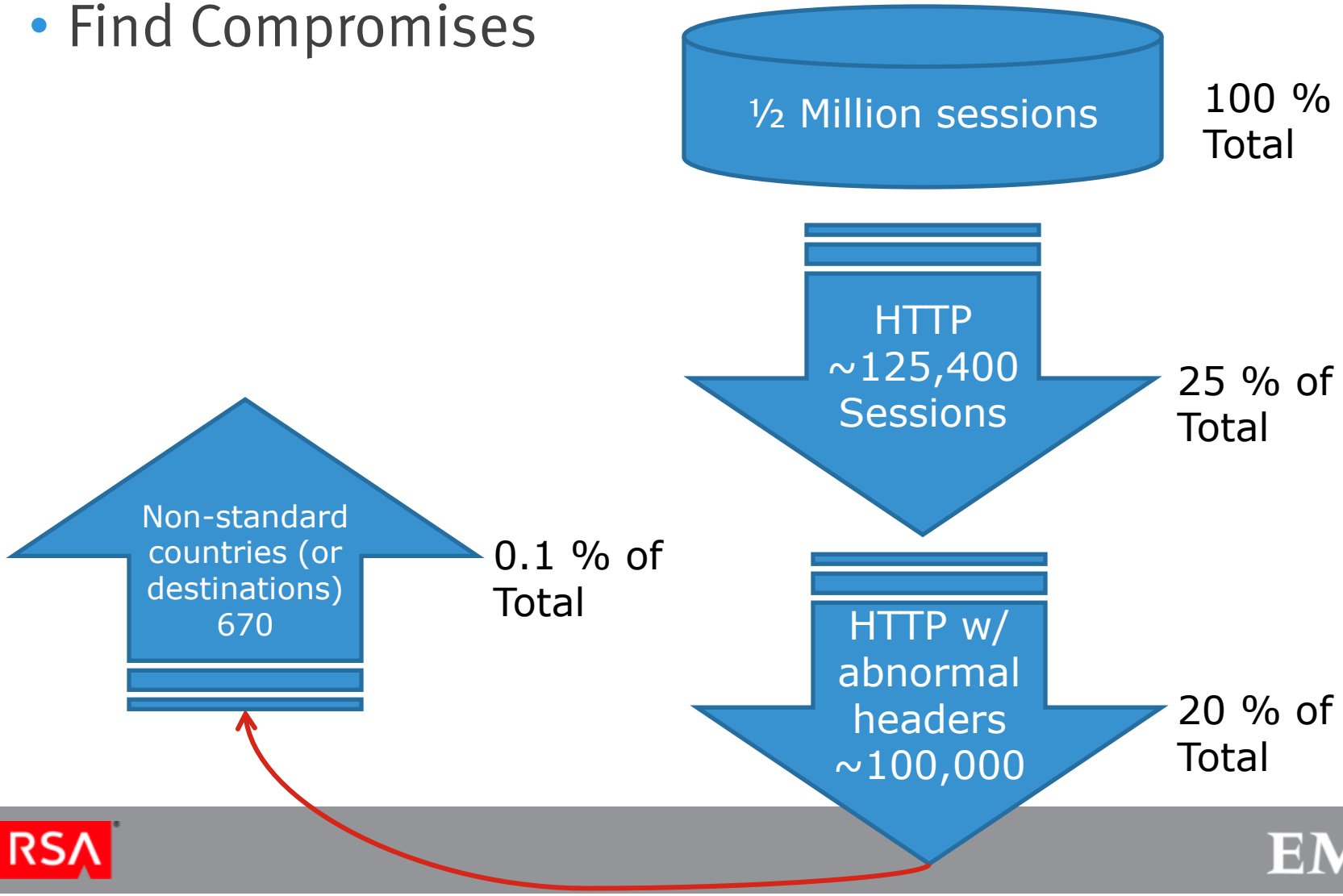
Example: Good network forensics

- Find Compromises



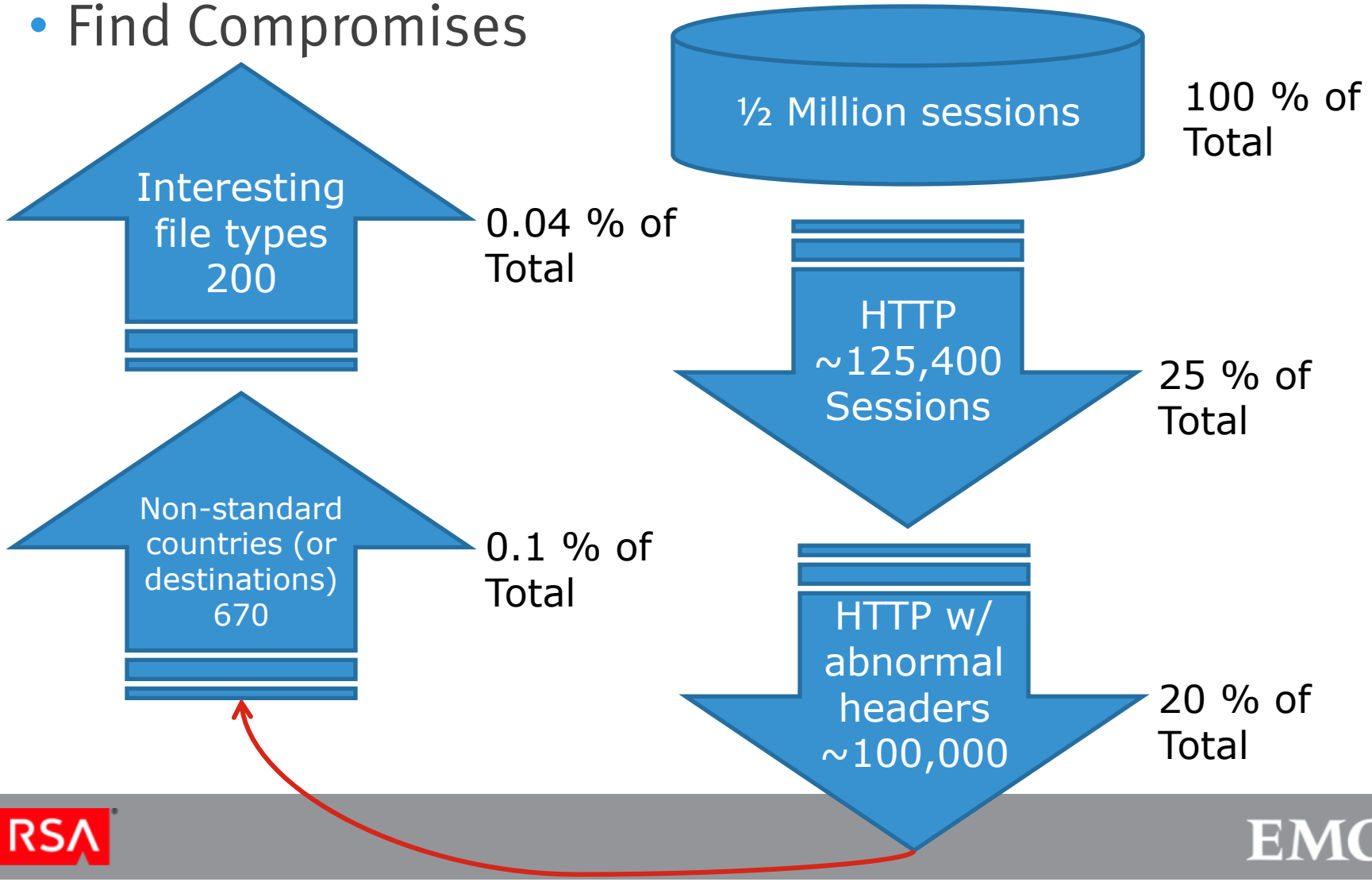
Example: Good network forensics

- Find Compromises



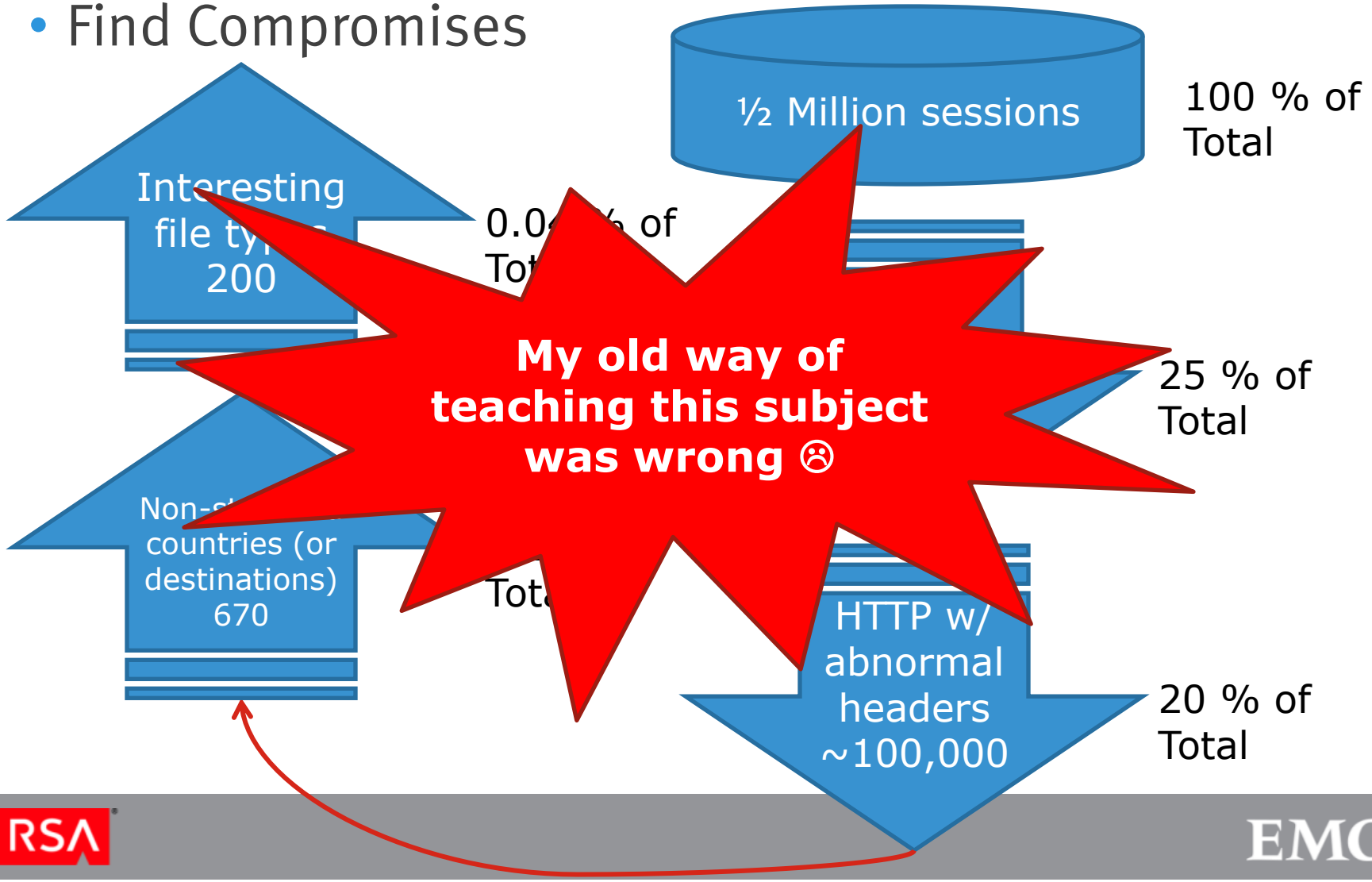
Example: Good network forensics

- Find Compromises



Example: Good network forensics

- Find Compromises



What network forensics really is

- Using “the needle in the haystack” analogy…

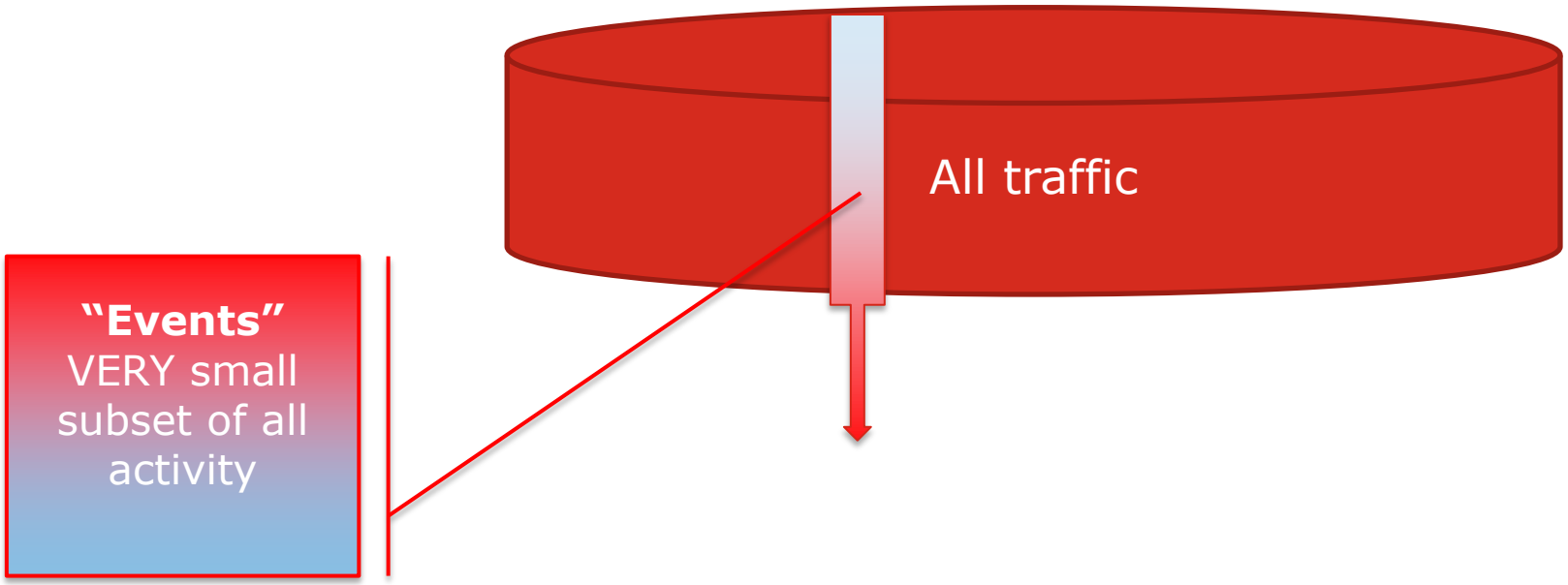
World-class forensics analysts remove hay until only needles remain

Why this is so important

- Traditional methods

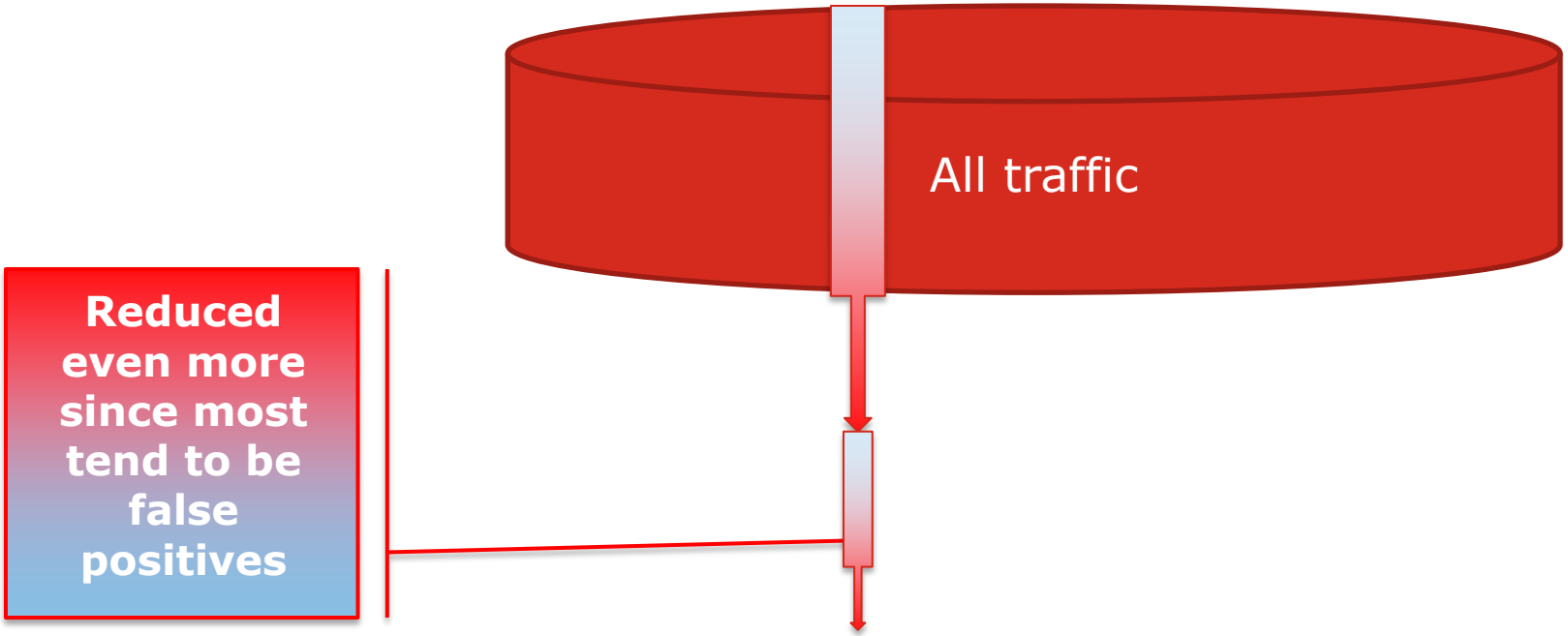
Why this is so important

- Traditional methods



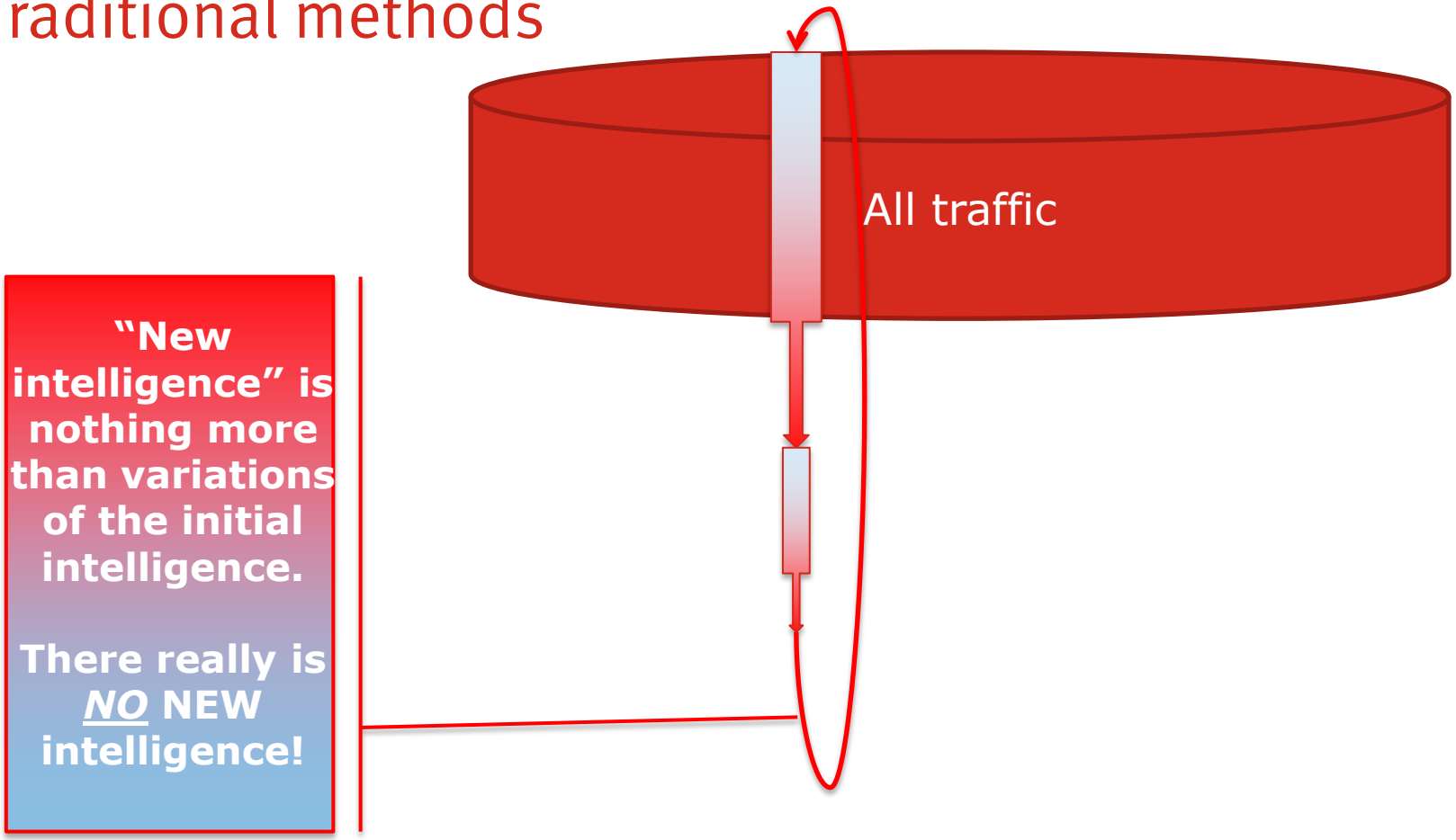
Why this is so important

- Traditional methods



Why this is so important

- Traditional methods



Why this is so important

- Traditional methods

"New intelligence" is nothing more than variations of the initial intelligence.

There really is *NO* NEW intelligence!

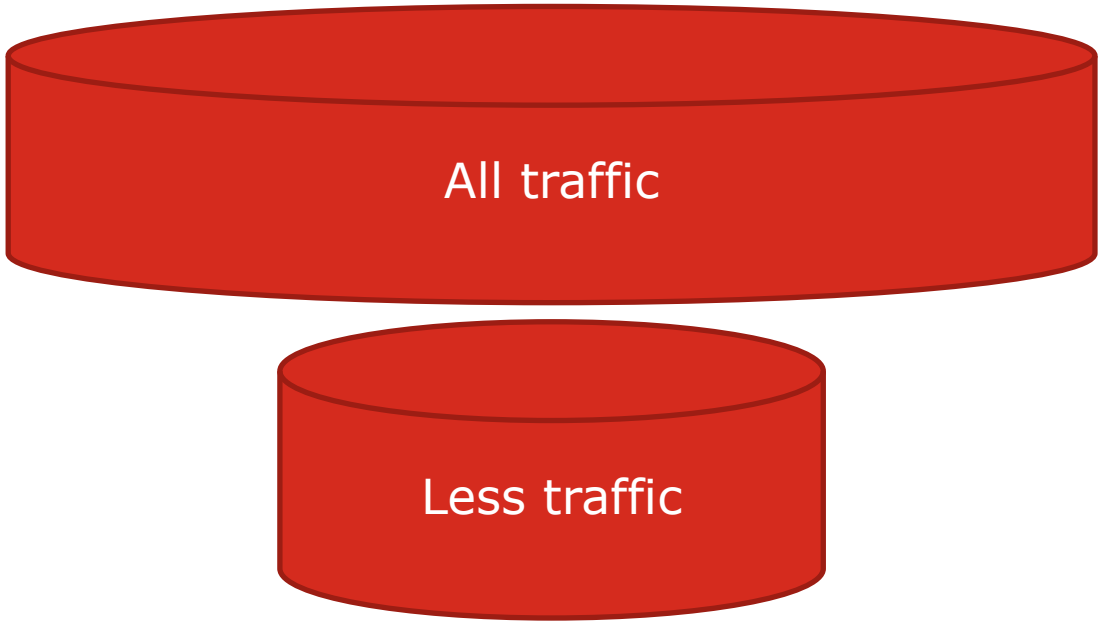
This is why accuracy of security products has been on a rapid decline over the past decade

Why this is so important

- Real Forensics

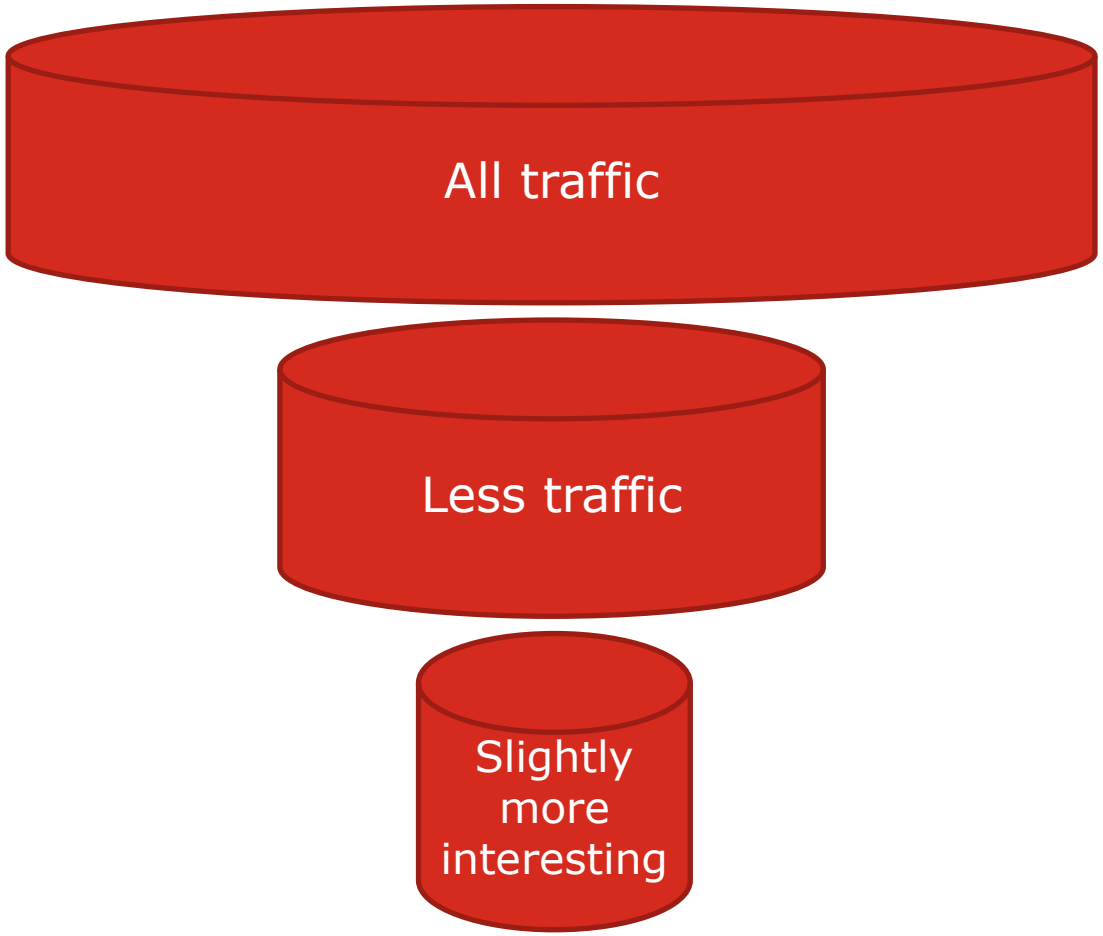
Why this is so important

- Real Forensics



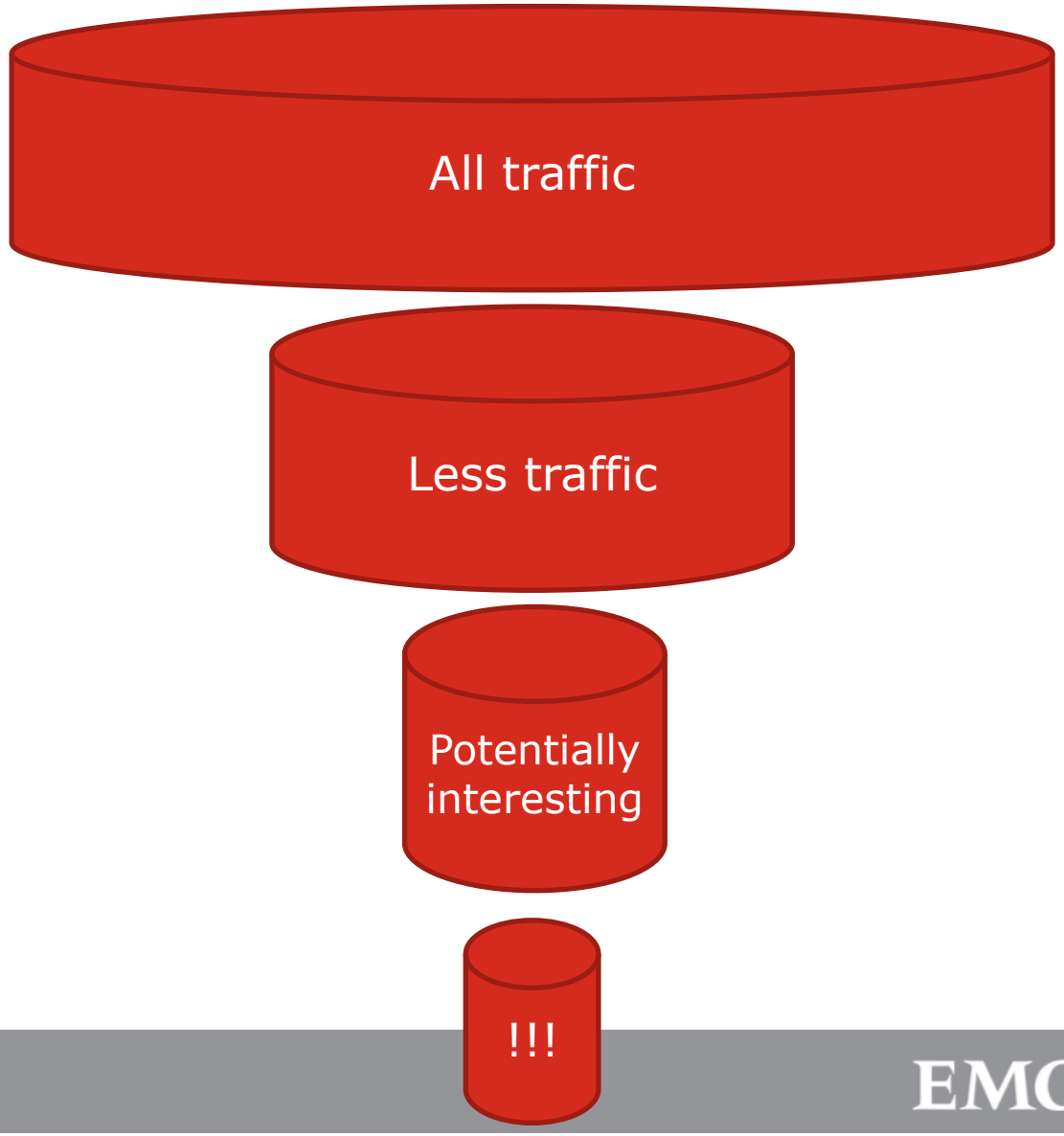
Why this is so important

- Real Forensics



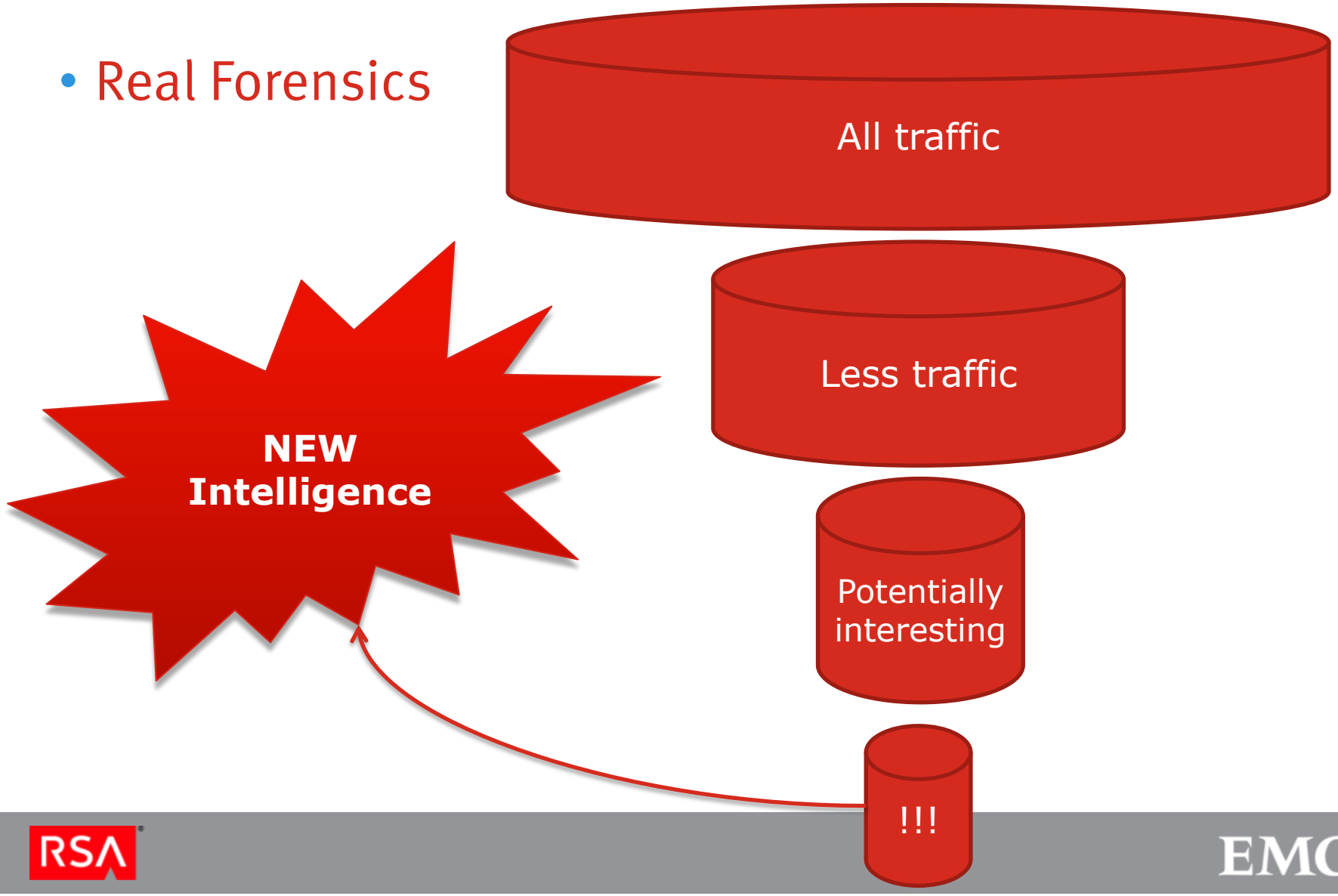
Why this is so important

- Real Forensics



Why this is so important

- Real Forensics



LEARN THIS!

- **The entire purpose to becoming a world class analyst is to generate new intelligence**

- Analysis is tedious.
- You should NOT be repeating the same processes to find the same things
- New intelligence is used to automate finding those [now] known threats in the future (which is not forensics at that point)
- **So you can continue focusing on finding new unknown threats!!!**

The Dynamic Approach to Security Analysis

The process of separating "normal" activity to discover "interesting" activity - for the *primary* purpose of generating new "intelligence."

- *Leverage new intelligence by building content to affect automation…*

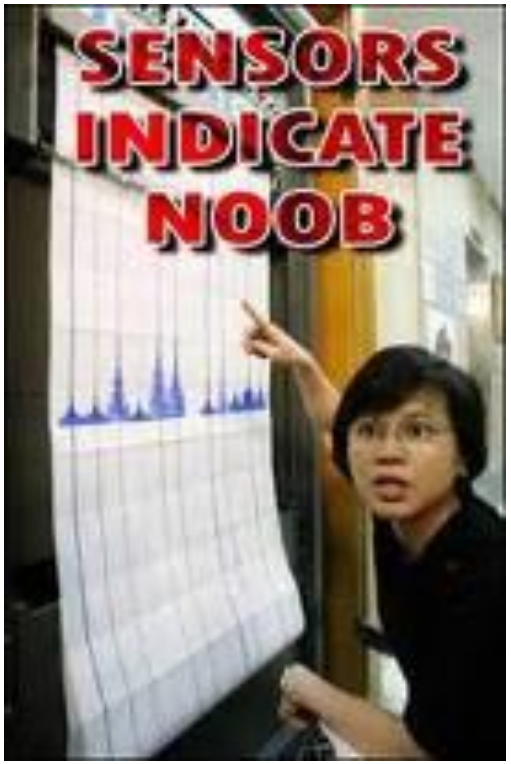
Touching The Void

AKA, How to Remove Hay

Indicators

- A threat indicator is a condition that, when present, increases the possibility of an incident.
- An indicator is a "piece of the puzzle". In other words, an indicator is any piece of information that can be exploited to gain further information, or be combined with other indicators to build a more complete profile of your operations or those of your adversary.

Indicators



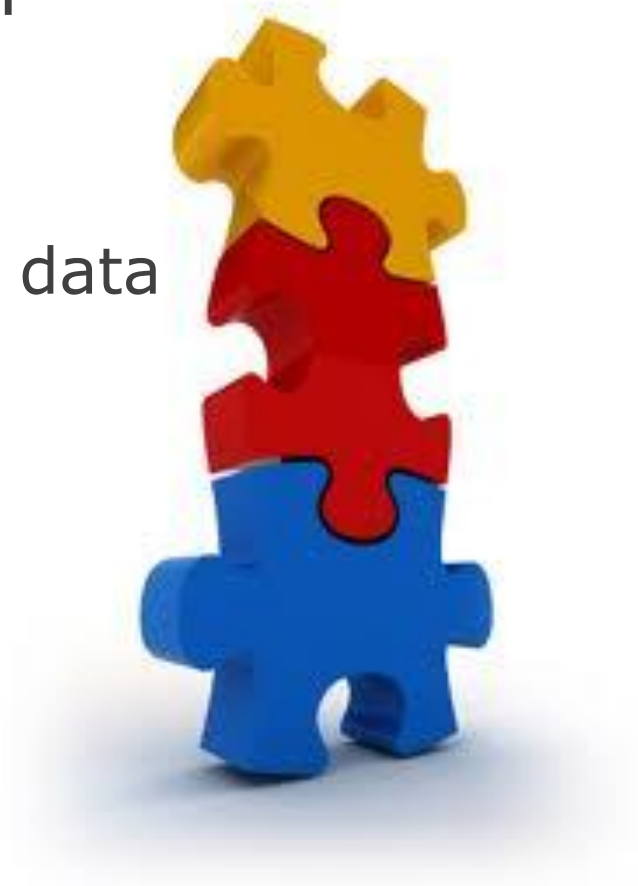
- Trait that points to an event
- Monitor to indicate an occurrence of a phenomenon
- Constantly review
  - Prune
  - Create
- Choose indicators wisely
- Poor indicators lead to analytic failure

Indicator Goals

- Observable and collectable
  - If it's not observable or observed it's worthless
  - If you expect to do trending it must be collected
- Valid
  - Relevant to the end state you're trying to predict
  - Must be inconsistent with events that don't match that pattern
- Reliable
  - Should point to the same event constantly
- Stable
  - Useful over time
- Unique
  - Measure one thing
  - Point to unique events when combined with other indicators

Creating Methodologies

- Putting the pieces together
  - Data harvesting
  - Data reduction
  - Reorganizing and search of data
  - Analysis of data
  - Reporting



Analysis Methodologies

Workflows

- Activity Identification
  - Example: Compromise
- Relationship Identification
  - Spider out for more information

Analysis

- Baseline
- Timeline
- Pathological
- Behavioral

Baseline Analysis

- "Now vs. Then"
- Answers the question *"Has there been change?"* or *"What changed?"*
- A baseline, in simplest terms, is merely a point from which to begin the process of analysis, and provides a reference against which to measure.

Temporal Analysis

- Provides context relative to the timeline of a system or events
- Often used to establish boundaries of the analysis window, and of critical importance in establishing the progression of events related to *The Event*

Pathological Analysis

- Establishes any variation or deviation from "normal"
- Decomposes the "*how*" of change.
- Described as "*the science of things that aren't so.*"
  - Park, Robert (2000). Voodoo Science: The Road from Foolishness to Fraud. Oxford University Press. ISBN 0-19-860443-2.

The Right Questions… Are they important?

"If they can get you asking the wrong questions, they don't have to worry about answers."

Thomas Pynchon, Gravity's Rainbow

What are some of the questions going unanswered?

- Do we have the kind of intelligence-gathering and analysis capabilities that we need to keep up with the threats?
- Is our security monitoring program actually looking for the right things?
- Would attackers be able to hijack administrative accounts?
- How many of our users would fall prey to a spear-phishing attack?
- Do we have what it takes to fully leverage threat information from other organizations?

Lex Parsimoniae

- Occam's Razor
  - " All else being equal, a simpler explanation is better than a more complex one."
- The more sophisticated the technology the more vulnerable it is to primitive attacks. People often overlook the obvious.
- Low-tech attacks work (even against high-tech devices and systems).
  - *Case in Point: The RSA Breach*
- Stay out of the weeds until you have eliminated all of the obvious answers

Analyze Threats

- Generally, threats can be analyzed based upon…
  - Who
    - *Who is conducting and/or directing attacks?*
  - What
    - *What specific organizations and information assets are they targeting?*
  - Why
    - *What are their motives?*
  - How
    - *What tools, techniques, and procedures do the utilize?*

Analyze Vulnerabilities

- Look at your environment from the perspective of your adversaries...
- What are the vulnerabilities in software/hardware that could make you prone to attack?
- Are there specific vulnerabilities in your systems that are open to potential exploit by your adversaries?
- Recognize that these vulnerabilities represent opportunities for your adversaries to capitalize on.
- *Your knowledge of the organization's mission, success criteria, and operations directly affect your capability to analyze your vulnerabilities.*

Assess Risks

- Align vulnerabilities with threats and assign risk levels.
- Risk = probability × impact
  - Where
- Probability = threat × vulnerability

- Decomposes to:
- ***Risk = threat × vulnerability × impact***

In Summary…

- Today's threats are dynamic and increasing in sophistication, requiring a fresh and more comprehensive approach to defense
- Advanced Threats are increasingly targeting corporations and governments in order to conduct industrial espionage, undermine business and financial operations, and/or sabotage infrastructure.
- The hard truth is that most organizations don't know enough about the threats or their own security posture to defend themselves adequately against the rising tide of cyber attacks.
- Successful defense against contemporary threats requires evolving past conventional approaches in information security.

Next Steps

- The industry agrees:
  - Download the latest RSA Security Brief here:
  - http://www.emc.com/collateral/software/solution-overview/h11031-transforming-traditional-security-strategies-so.pdf
  - Industry experts assert that today's latest threat landscape requires an evolution of SIEM systems and perimeter-focused defenses to gain better visibility, agility, and speed into complex IT environments.
- Attend "Why Logs Are Not Enough" webcast on October 17 at 2:00 ET. Register now: https://emcinformation.com/93207/REG/.ashx

THANK YOU

QUESTIONS?


RSA


EMC²