Security in knowledge

Why can’t you get what I’m saying?

Penetrating the mental firewall

David Porter

Resilient Thinking

RSACONFERENCE
EUROPE 2013

Session ID: HUM-W10

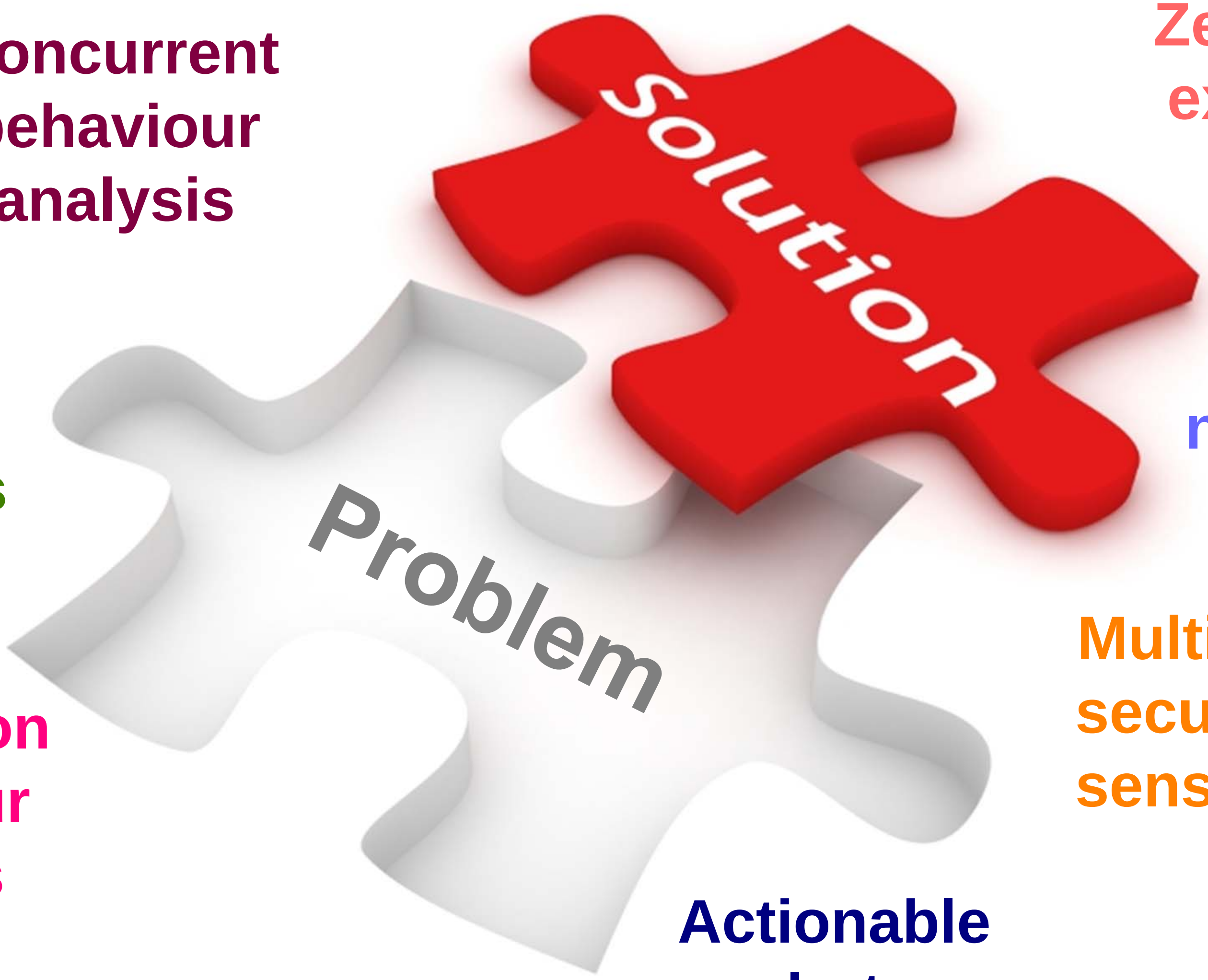
Session Classification: General interest

Structured fluidity

You're the security expert

Concurrent behaviour analysis

Zero-day exploits



Static indicators

False negatives

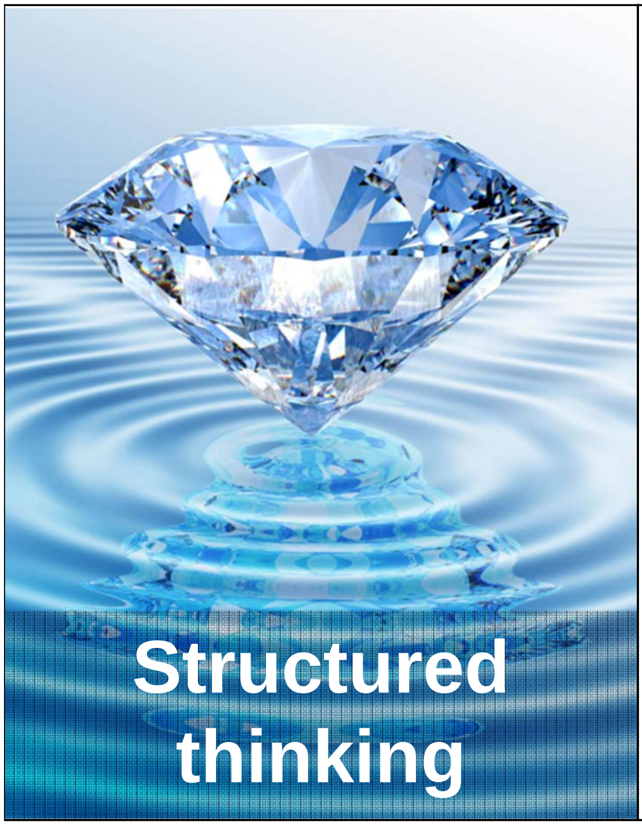
Application behaviour analysis

Multiple security sensors

Actionable alerts

But they won't listen

Coming up…



Structured thinking

Clearly compelling

Persuasive deception

Structured thinking

Security in knowledge

#RSAC

RSACONFERENCE
EUROPE 2013

“On-grid”: chaotic, distractive writing

“Don‘t worry about the structure, just get all the words down and we’ll clean it up afterwards ”

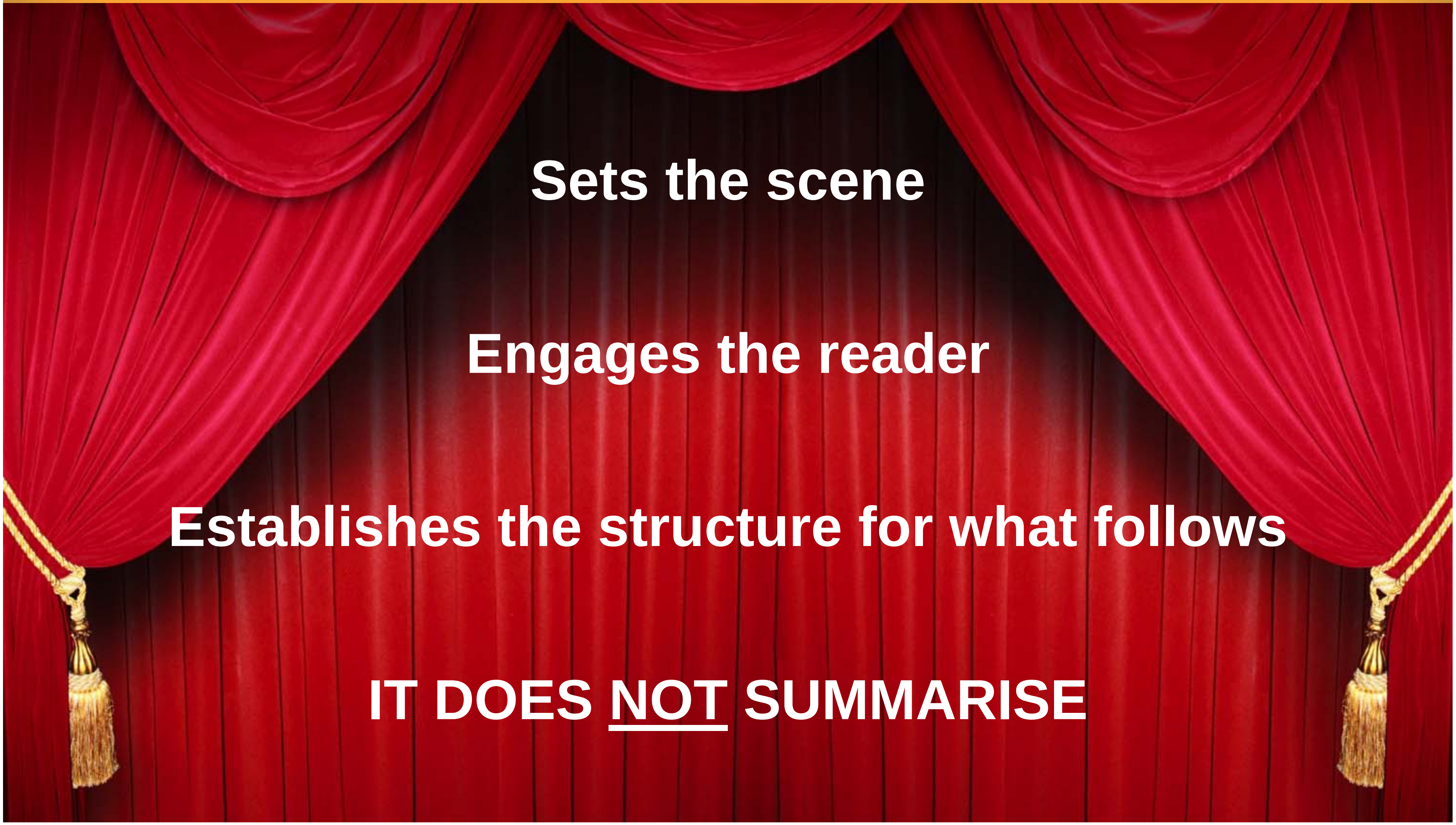
— Information Security Senior Executive

Source: http://www.henderson-art.co.uk/art-detail.php?id=chaos

"Off-grid": structured thinking

The introduction

What is an introduction?



Sets the scene

Engages the reader

Establishes the structure for what follows

IT DOES NOT SUMMARISE

We all love stories

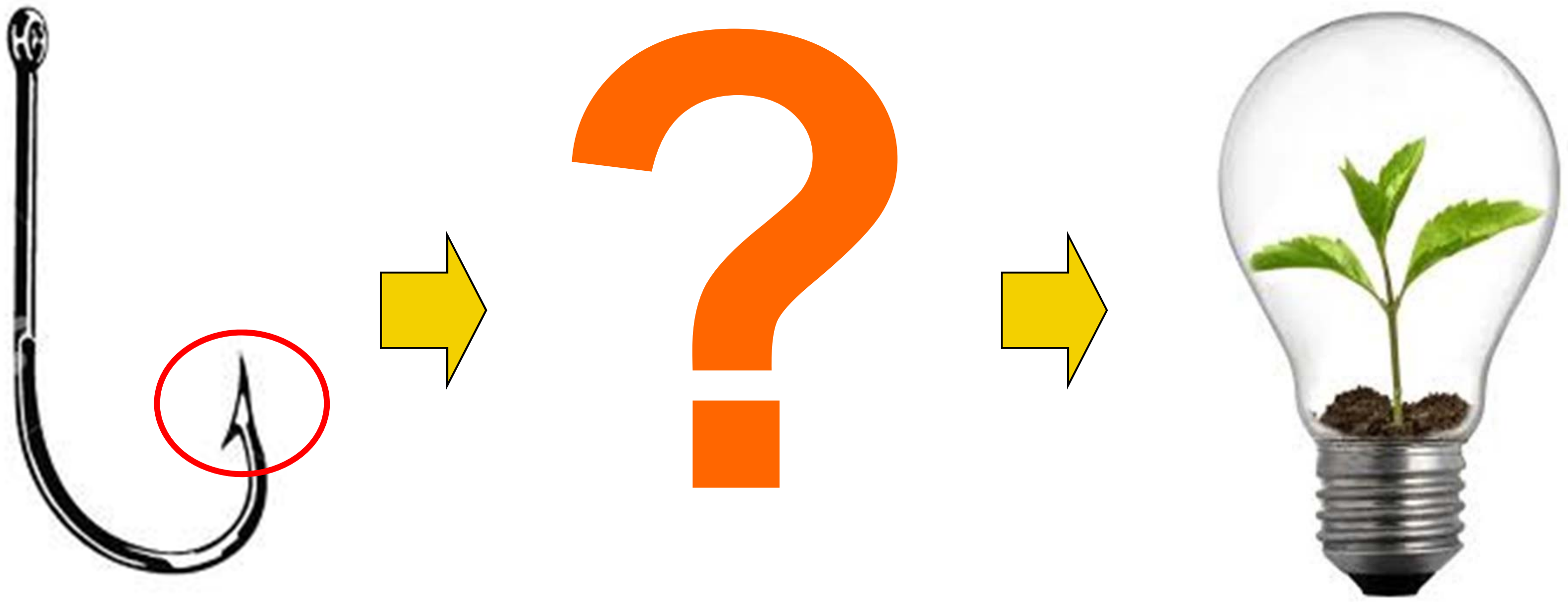
Situation

Once upon a time there lived a lovely little Princess named Snow White.

Her vain and wicked Stepmother the Quee ared that some day Snow Whi eauty would surpass her own. S e dressed the little Princess in rags forced her to work as a Scullery Maid.

Complication

Story-based introduction structure



Situation

Complication

(Question)

Answer

Source: Barbara Minto, The Pyramid Principle: Logic in Writing and Thinking

Anatomy of a great introduction

Welcome to a universe of Big Data, the next wave in Information Technology. One of the impediments to achieving success in this next wave is Trust. Privacy is a big piece of that Trust. The security industry needs a scalable ecosystem for sharing information beyond the current industry models that leverages existing trusted relationships and Big Data. Big Data has the potential to transform our lives for the better; our health, environment, our livelihood, almost every facet of our daily lives. Big Data is more than just a whole lot of data. It's the ability to extract meaning: to sort through the masses of data elements to find the hidden pattern, the unexpected correlation, the surprising connection. Did you know the volume of information in the world is doubling every two years and less than one percent of the world's data is analyzed, and less than 20 percent of it is protected? Art Coviello will discuss how Big Data is transforming information security and how an Intelligence-driven security strategy that uses the power of big data analytics will put the advantage of time back on the side of security practitioners enabling them to detect attacks, respond more quickly and reduce attacker dwell time.

Situation **Complication**

Anatomy of a great introduction

Welcome to a universe of big data, the next wave in information technology. Big data has the potential to transform our lives for the better: our health, our environment and our livelihood — almost every facet of our daily lives.

But one of the impediments to achieving success in this next wave is trust. While the volume of information in the world is doubling every two years, less than one percent of the world's data is analyzed and less than 20 percent of it is protected. Privacy is a big piece of that trust.

?

Situation **Complication**

Other great RSA introductions

In the past, application security professionals thought firewalls, SSL, patching, and privacy policies were enough. Today, however, these methods are outdated and ineffective, as attacks on prominent, well-protected applications are occurring every day…

Data drives decisions for business leaders on a daily basis - whether it's for routine daily tasks, or for the most strategic and impactful actions. But CSOs are typically policy-driven and have few data sources to depend on...

Situation **Complication**

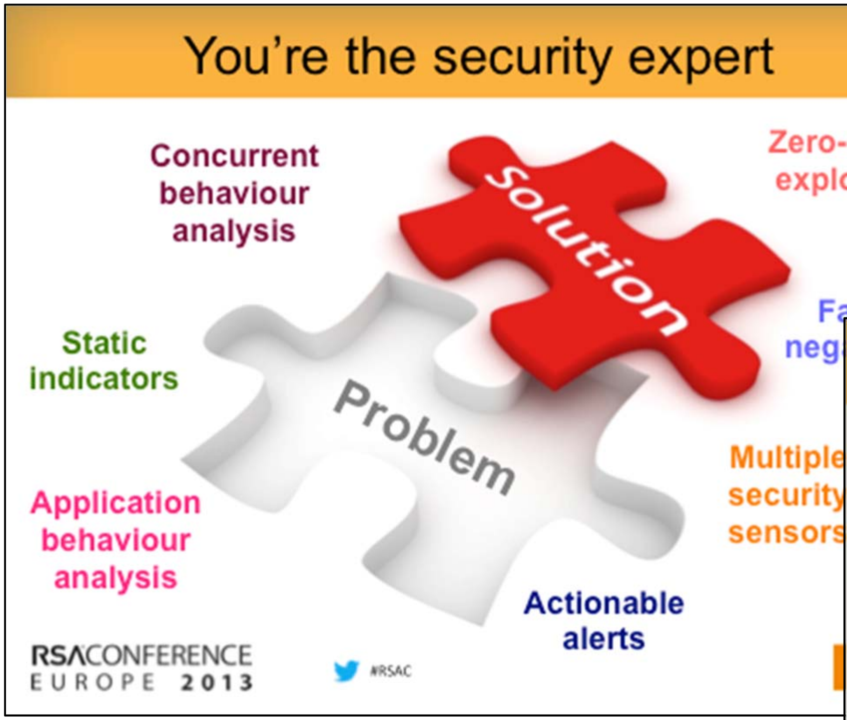
80% of companies are already experiencing the "Bring Your Own Device" trend (BYOD). Yet less than half of these companies actually do something about the security risks it introduces…

Computer chip performance has doubled every two years and HDD capacity has scaled even faster. But Authentication hasn't scaled. Cloud services still see users tortured with usernames and passwords...

Two-factor authentication (2FA) requirements are well defined. But the standard approach requiring distribution of factors can slow adoption...

Source: Rolf Lindemann, Nok Nok Labs Inc., "Scalable Authentication"

This afternoon's introduction



You're the security expert

Concurrent behaviour analysis

Zero-day exploits

Static indicators

False neg

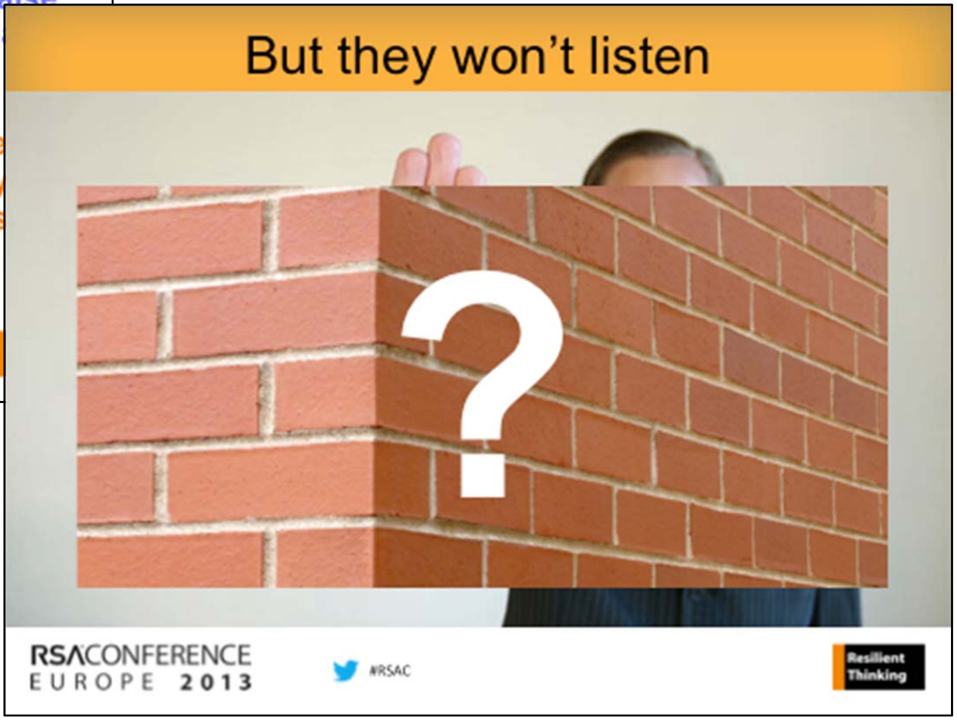
Multiple security sensors

Application behaviour analysis

Actionable alerts

Solution
Problem

RSACONFERENCE EUROPE 2013 #RSAC



But they won't listen

RSACONFERENCE EUROPE 2013 #RSAC Resilient Thinking

Find your complication

Beyond the introduction

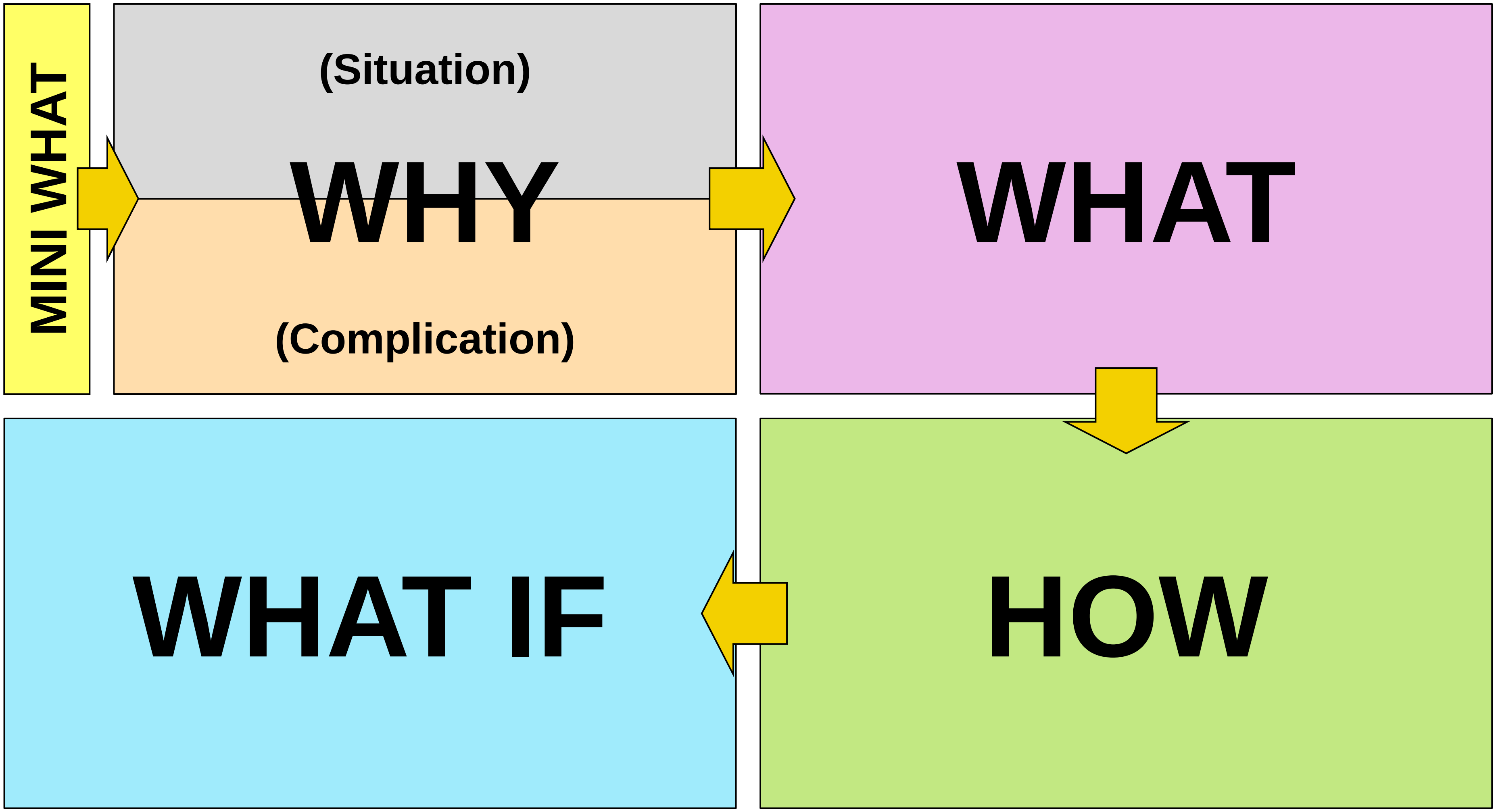
Difference?

SAML is widely implemented by enterprises due to its robust security characteristics. Its primary use is for Web SSO between users and services. With success of the SaaS delivery model, OAuth is rapidly gaining momentum for securing access to web resources via APIs. This session reviews the complementary features of these two standards and explores multiple hybrid use cases for the enterprise.

Security professionals have reached a turning point where the technologies and methods of the past are no longer enough. In order to meet the increasingly sophisticated attacks of today, companies must take a more proactive stance through the use of actionable intelligence. Only by fusing relevant corporate data with global intelligence can we actually identify threats, prioritize efforts and ultimately protect our most critical assets.

Back to school

Learning styles/information needs



MINI WHAT

(Situation)

WHY

(Complication)

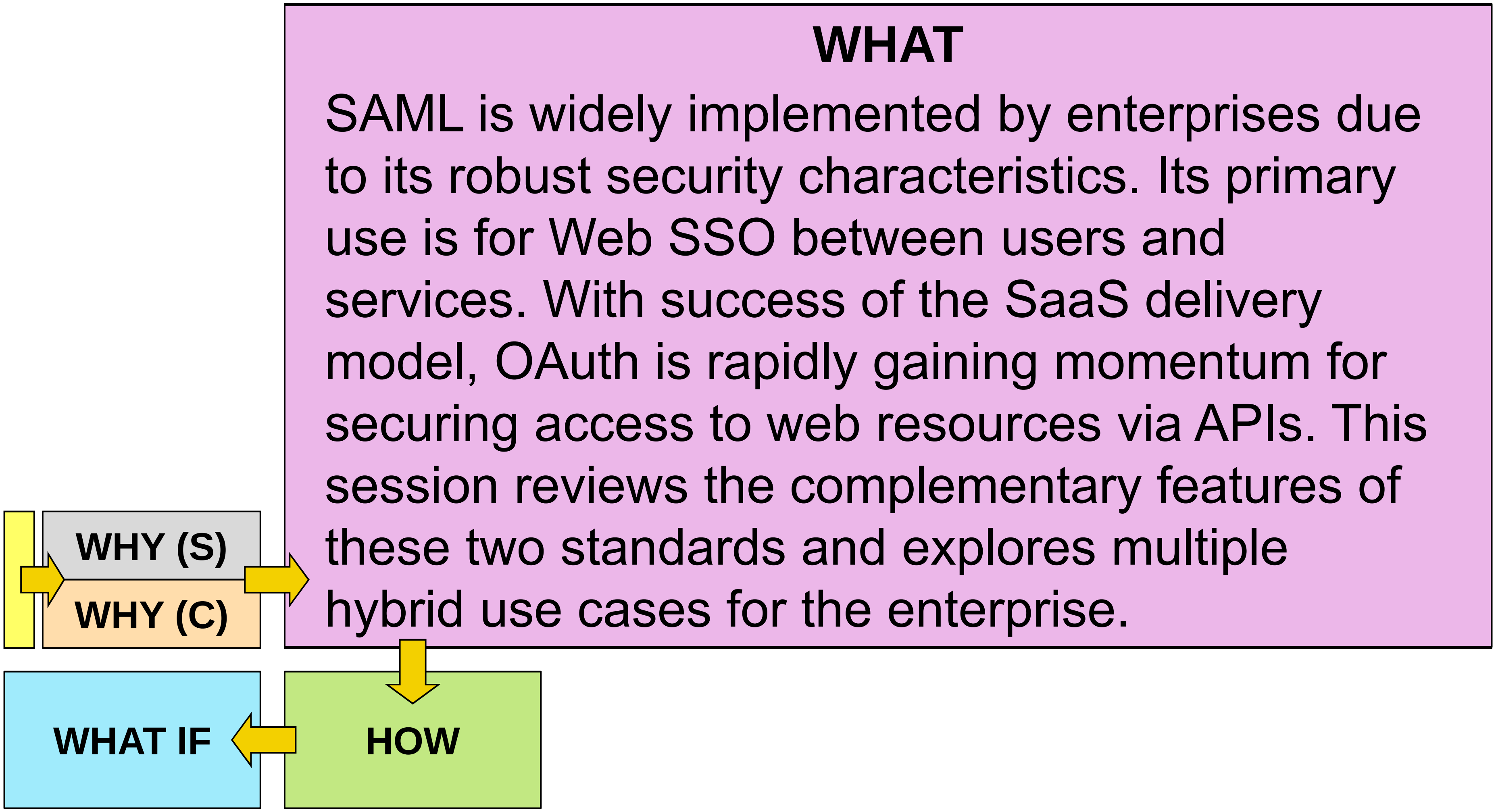
WHAT

HOW

WHAT IF

Source: Bernice McCarthy, About Teaching:
4MAT in the Classroom

Focusing on the "what"



WHAT

SAML is widely implemented by enterprises due to its robust security characteristics. Its primary use is for Web SSO between users and services. With success of the SaaS delivery model, OAuth is rapidly gaining momentum for securing access to web resources via APIs. This session reviews the complementary features of these two standards and explores multiple hybrid use cases for the enterprise.

Understanding the difference

SAML is widely implemented by enterprises due to its robust security characteristics. Its primary use is for Web SSO between users and services. With success of the SaaS delivery model, OAuth is rapidly gaining momentum for securing access to web resources via APIs. This session reviews the complementary features of these two standards and explores multiple hybrid use cases for the enterprise.

Security professionals have reached a turning point where the technologies and methods of the past are no longer enough. In order to meet the increasingly sophisticated attacks of today, companies must take a more proactive stance through the use of actionable intelligence. Only by fusing relevant corporate data with global intelligence can we actually identify threats, prioritize efforts and ultimately protect our most critical assets.

Why	S	C	What
What if			How

Anatomy of the main body

Welcome to a universe of Big Data, the next wave in Information Technology. One of the impediments to achieving success in this next wave is Trust. Privacy is a big piece of that Trust. The security industry needs a scalable ecosystem for sharing information beyond the current industry models that leverages existing trusted relationships and Big Data. Big Data has the potential to transform our lives for the better; our health, environment, our livelihood, almost every facet of our daily lives. Big Data is more than just a whole lot of data. It's the ability to extract meaning: to sort through the masses of data elements to find the hidden pattern, the unexpected correlation, the surprising connection. Did you know the volume of information in the world is doubling every two years and less than one percent of the world's data is analyzed, and less than 20 percent of it is protected? Art Coviello will discuss how Big Data is transforming information security and how an Intelligence-driven security strategy that uses the power of big data analytics will put the advantage of time back on the side of security practitioners enabling them to detect attacks, respond more quickly and reduce attacker dwell time.

Why	S	C	What
What if			How

“Big data needs BIG SECURITY”

Welcome to a universe of big data, the next wave in information technology. Big data has the potential to transform our lives for the better: our health, our environment and our livelihood — almost every facet of our daily lives.

But one of the impediments to achieving success in this next wave is trust. While the volume of information in the world is doubling every two years, less than one percent of the world's data is analyzed and less than 20 percent of it is protected. Privacy is a big piece of that trust.

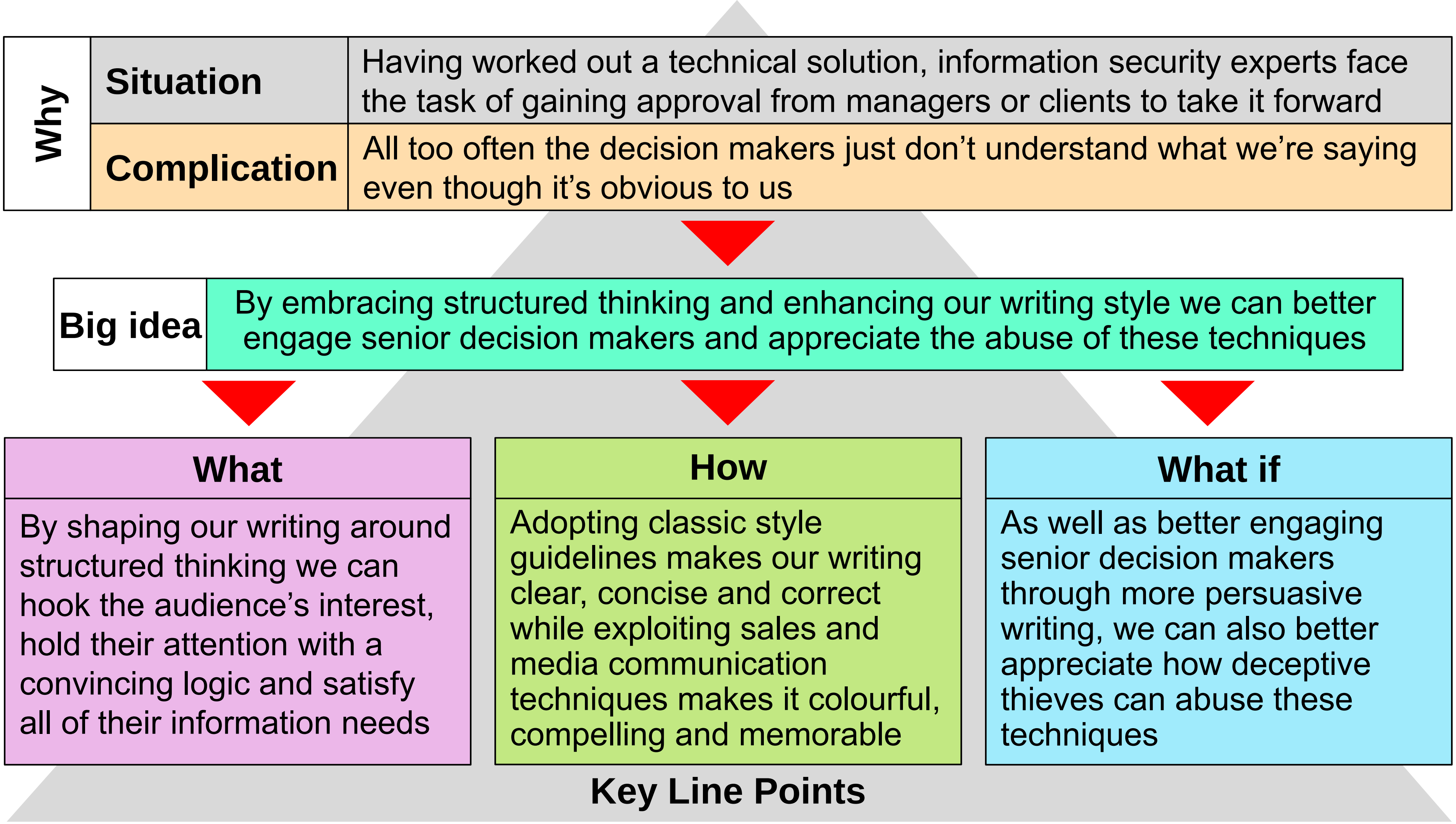
Art Coviello will discuss how big data is transforming information security and how it is more than just a whole lot of data. It's the ability to extract meaning: to sort through masses of data elements to find the hidden pattern, the unexpected correlation, the surprising connection.

Art will explain how the security industry needs a scalable ecosystem for sharing information — going beyond current industry models — that builds on existing trusted relationships.

An intelligence-driven security strategy will exploit the power of big data analytics and put the advantage of time back on the side of security practitioners. This will enable them to detect and respond to attacks more quickly and reduce attacker dwell time.

Why	S	C	What
What if			How

Composite model (simplified)



Why		
	Situation	Having worked out a technical solution, information security experts face the task of gaining approval from managers or clients to take it forward
	Complication	All too often the decision makers just don’t understand what we’re saying even though it’s obvious to us

Big idea By embracing structured thinking and enhancing our writing style we can better engage senior decision makers and appreciate the abuse of these techniques

What	How	What if
By shaping our writing around structured thinking we can hook the audience’s interest, hold their attention with a convincing logic and satisfy all of their information needs	Adopting classic style guidelines makes our writing clear, concise and correct while exploiting sales and media communication techniques makes it colourful, compelling and memorable	As well as better engaging senior decision makers through more persuasive writing, we can also better appreciate how deceptive thieves can abuse these techniques

Key Line Points

It’s easy once you know how

As Smart TVs become more prevalent in waiting rooms and conference rooms, cybercriminals are learning to turn them into surveillance devices: they’re using them as instruments to steal money and secrets from businesses. Learn to stay a step ahead of the bad guys by understanding how they are getting in and how to stop them before they sit in on one of your meetings.

Why	S	C	What
How			What if

Source: Raimund Genes, Trend Micro, “How hackers are outsmarting smart TVs and why it matters to you”

A guide, not a straightjacket

Clearly compelling

Security in knowledge

Writing great words

Compelling

Clear, concise and correct

Clarity through brevity

“Je n'ai fait celle-ci plus longue parce que je n'ai pas eu le loisir de la faire plus courte.”

— Blaise Pascal, 17th Century ✓

“When forced to work within a strict framework the imagination is taxed to its utmost – and will produce its richest ideas. Given total freedom the work is likely to sprawl.”

— T.S. Eliot, 20th Century ✓

“It’s going to be hard to get any serious point across in 500 words.”

— Information Security Senior Executive, 21st Century ✗

Jargon

Leverage technology	Exploit technology
Drive security improvements	Improve security
Bi-manually controlled interception response	Using both hands

Obfuscation

Using our approach and this way of working we have achieved an end-to-end 100 day solution implementation timeframe to an initial release for this type of scenario

Using this approach we built a first release in 100 days

Simplicity

Purchase	Buy
Assist	Help
Additional	Extra
Approximately	About
In the event that	If
By means of	By
Due to the fact that	Because
For the purpose of	For

Spelling, gramm~~e~~ar and punctuation

It’s

Its

If you still persist in writing, 'Good food at it's best', you deserve to be struck by lightning, hacked up on the spot and buried in an unmarked grave”

— Lynne Truss

Source: Lynne Truss, Eats, Shoots & Leaves: The Zero Tolerance Approach to Punctuation

Being assertive and personal

Second order conditional (I would)	**Simple future tense** (I will)
Passive voice (The firewall was breached)	**Active voice** (I breached the firewall)
Impersonal (RSA is proud)	**Personal** (We are proud)

Assertive and personal

A range of security recommendations is proposed by the Security Department, from quick wins through to major initiatives. The Security Department team would discuss these with the Operations team after the report has been delivered.

We have proposed a range of security recommendations, from quick wins through to major initiatives. We will discuss these with you after we have delivered our report.

Keeping it really, really simple

A multilayer perceptron is a feedforward artificial neural network model that maps sets of input data onto a set of appropriate output. It is a modification of the standard linear perceptron, in that it uses three or more layers of neurons (nodes) with nonlinear activation functions, and is more powerful than the perceptron in that it can distinguish data that is not linearly separable, or separable by a hyperplane.

This more sophisticated form of data mining, known as "supervised learning", enables security risk models to be automatically derived on the basis of past case studies.

To teach a child what "red" means you just show them lots of red things. This technology is similar: you teach the computer by showing it lots of examples of security breaches so it can recognise new ones.

Using metaphor and imagery

Online exposure

Anomaly detection

Insider threat

Keep it simple

Persuasive deception

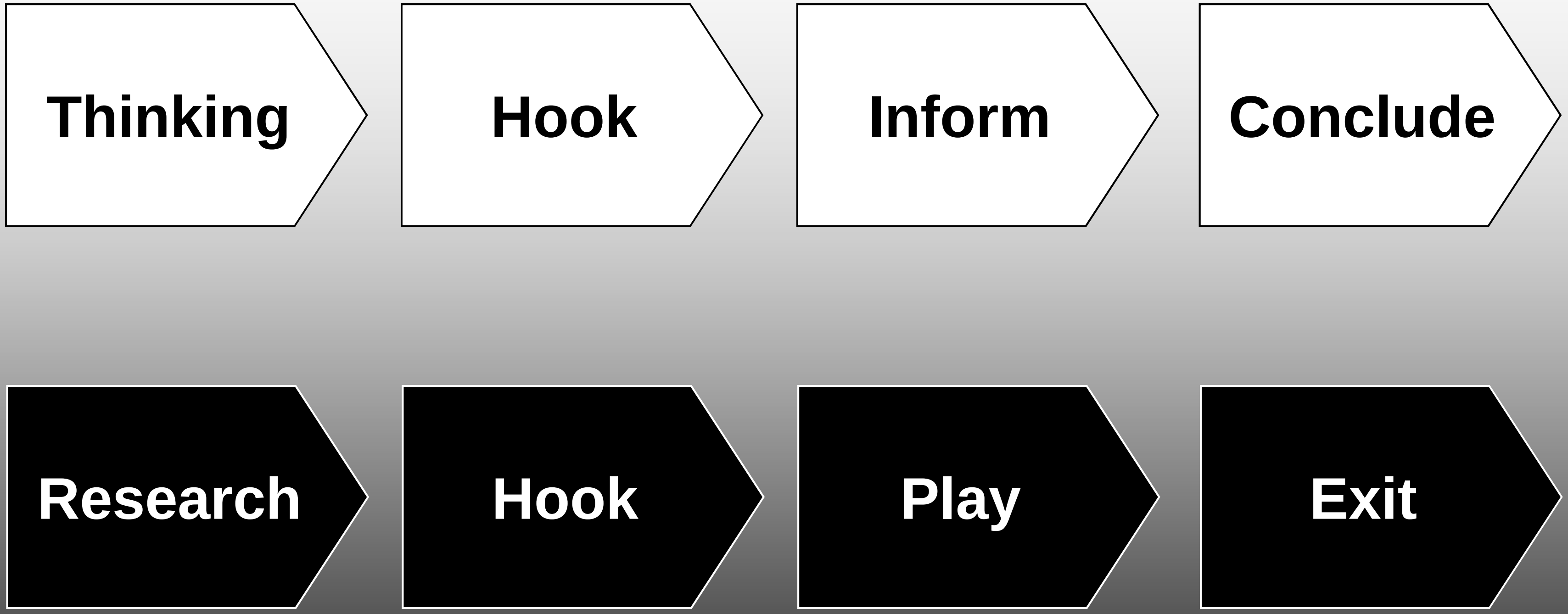
Security in knowledge

#RSAC

RSA CONFERENCE
EUROPE 2013

Penetrating mental firewalls

Convincing your boss/client/audience



Thinking → Hook → Inform → Conclude

Research → Hook → Play → Exit

Deceiving a victim (e.g. "spear phishing")

Pressing our "complication" buttons

Fear

Greed

Power

Pride

Sloth

Envy

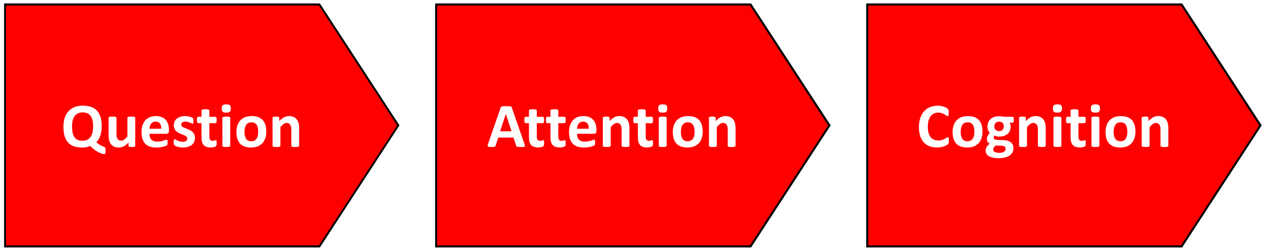
Wrath

Gluttony

Desire

Hooking with a question

Now the serpent was more subtle than any beast of the field which the LORD God had made. And he said unto the woman, “Yea, hath God said, Ye shall not eat of any tree of the garden?”



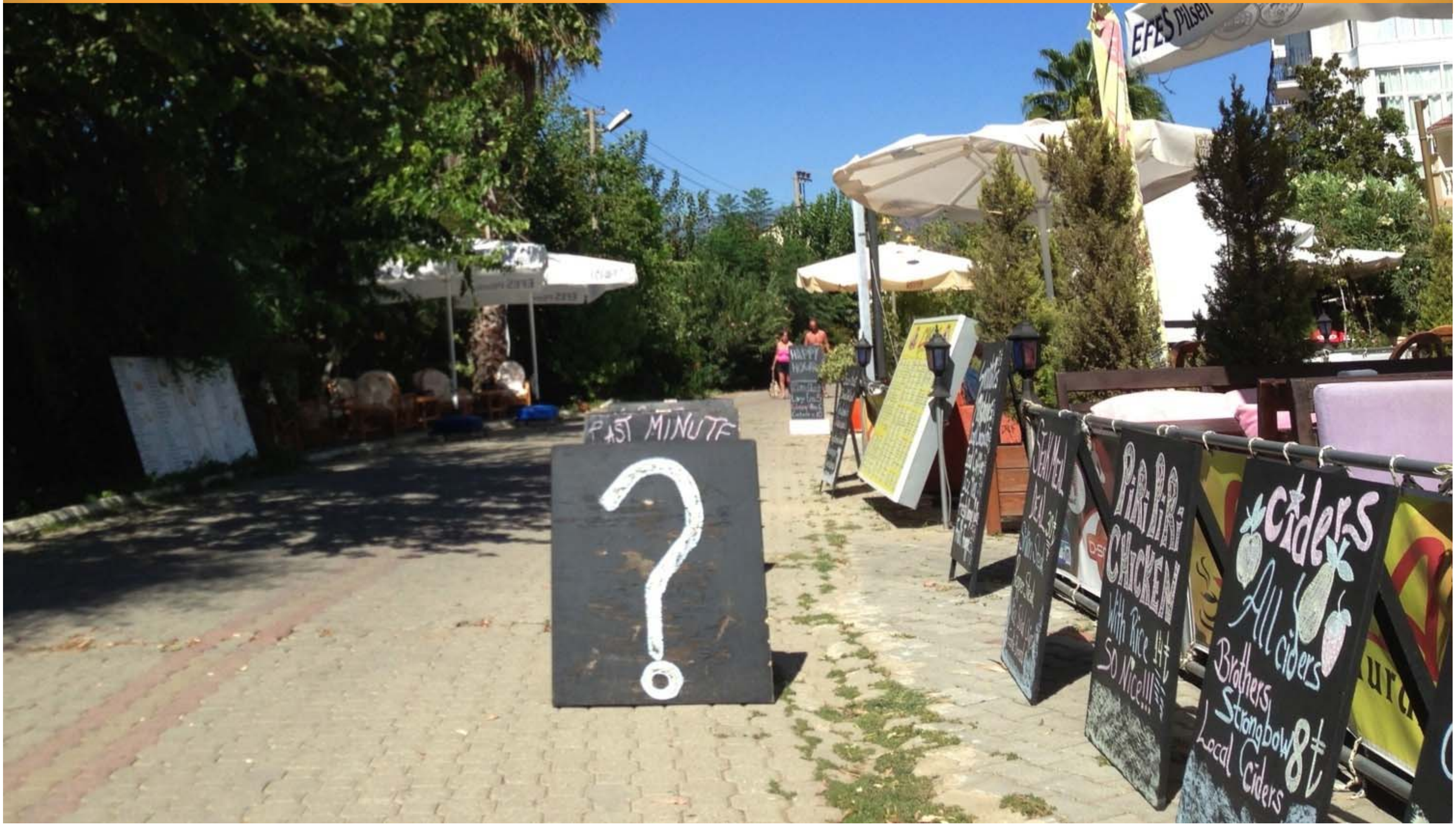
Question

Attention

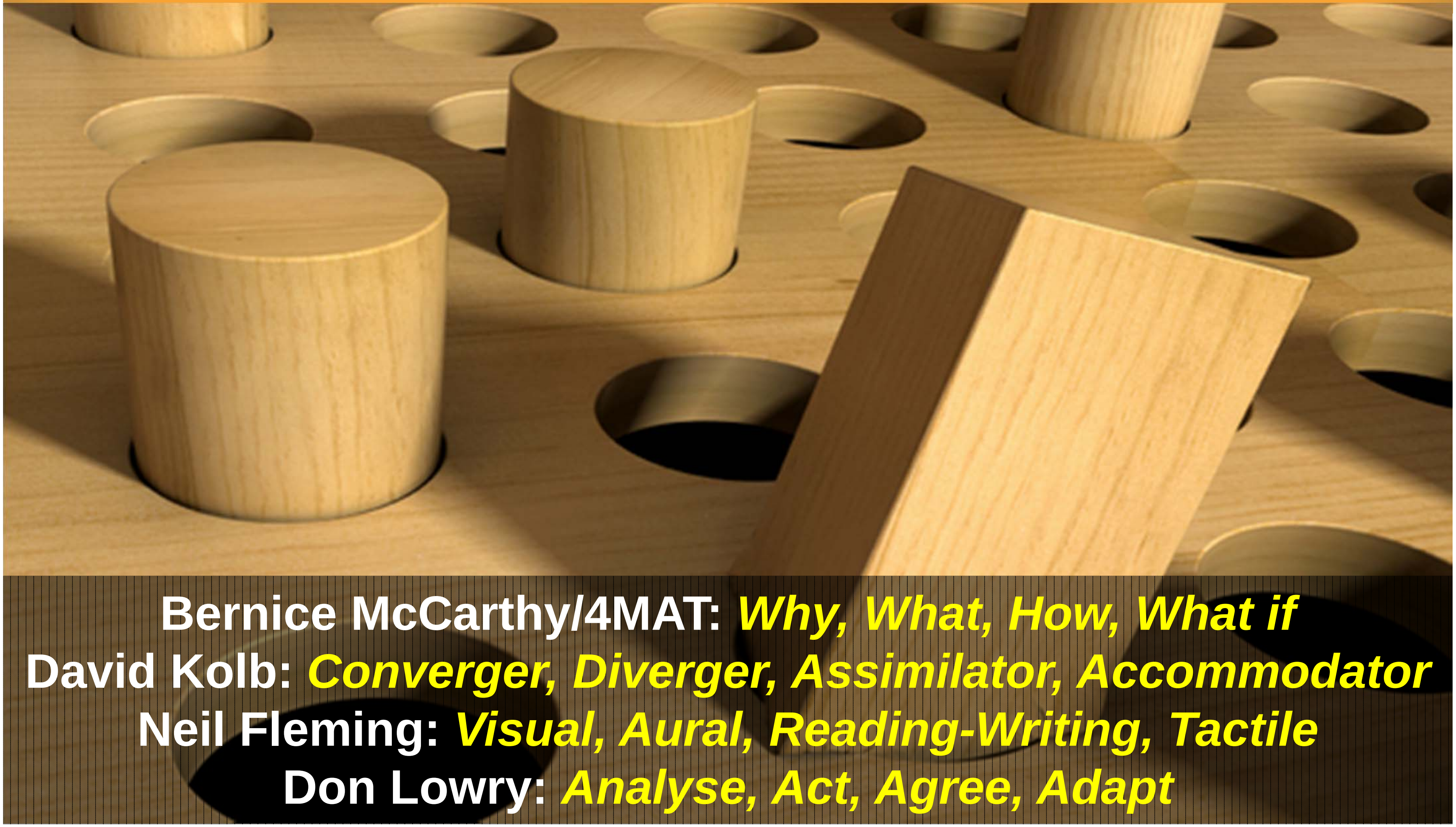
Cognition

Source: Genesis 3:1-6

Hooking with a question

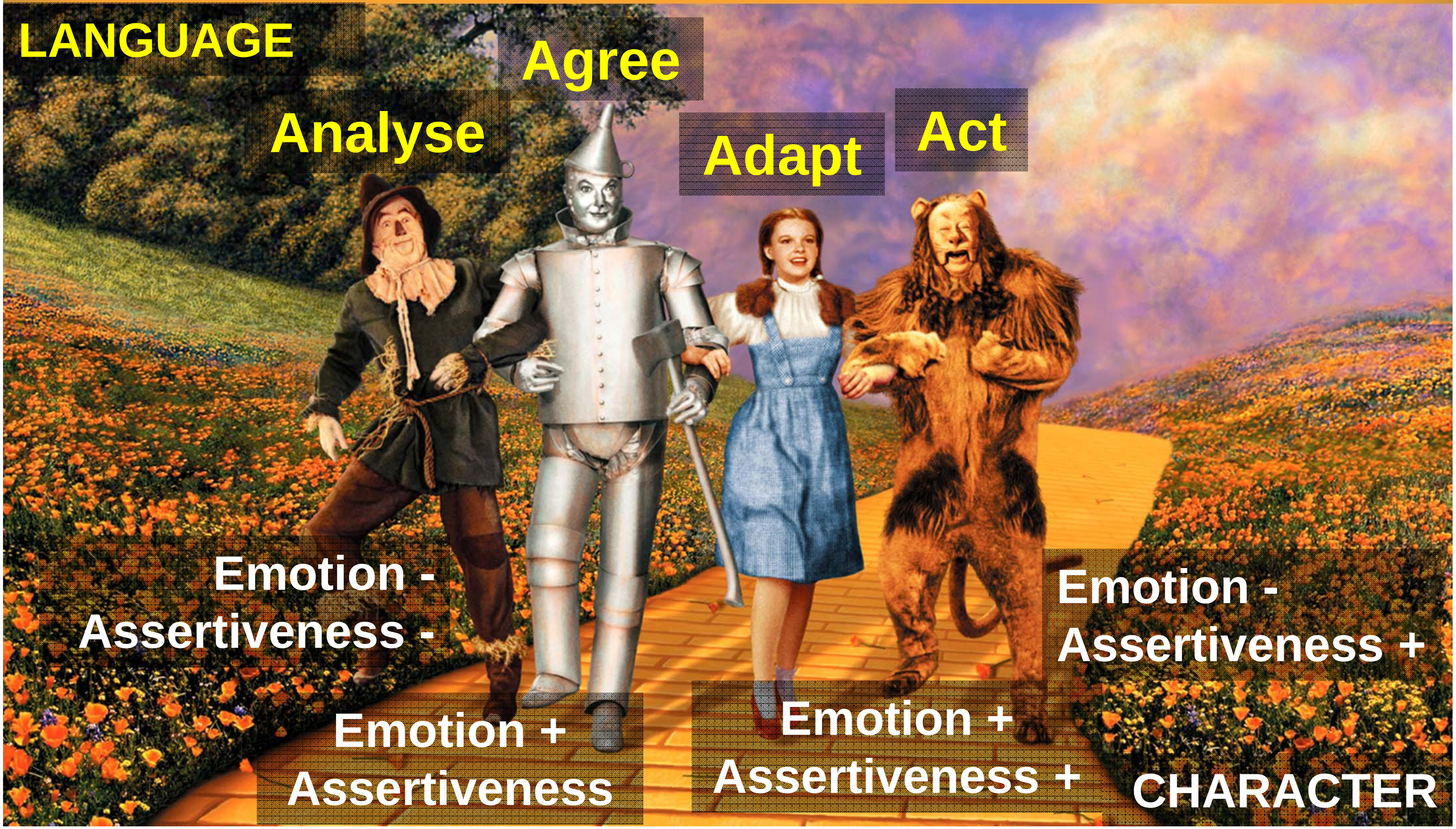


Delivering the message effectively



Bernice McCarthy/4MAT: ***Why, What, How, What if***
David Kolb: ***Converger, Diverger, Assimilator, Accommodator***
Neil Fleming: ***Visual, Aural, Reading-Writing, Tactile***
Don Lowry: ***Analyse, Act, Agree, Adapt***

Deceiving personalities with words



Beware literate serpents

In conclusion

Meet the McGuffin

“A McGuffin is nothing at all”

— Alfred Hitchcock

Examples of McGuffins

Concurrent behaviour analysis

Zero-day exploits

Microfilm

Secret formula

Static indicators

False negatives

Diamond necklace

Unobtanium

Multiple security sensors

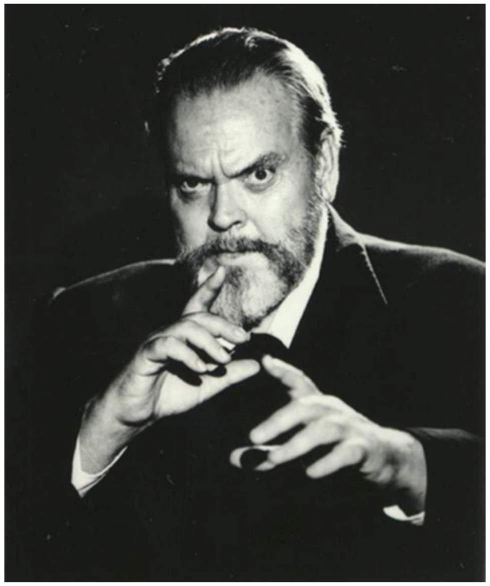
Application behaviour analysis

Actionable alerts

Security needs a story

“I can think of nothing that an audience won't understand. The only problem is to interest them; once they are interested, they understand anything in the world”

— Orson Welles



Find your complication

Keep it simple

Beware literate serpents

Application

Applying today's lessons

Create a structured introduction next time you write something

Refresh awareness training to include literate serpents

Visit people in Marketing to swap ideas

Some useful information

- “The Pyramid Principle: Logic in Writing and Thinking” by Barbara Minto
- “Eats, Shoots & Leaves: The Zero Tolerance Approach to Punctuation” by Lynne Truss
- “Practical English Usage” by Michael Swan
- GOV.UK Style Guide: https://www.gov.uk/designprinciples/styleguide

Security in knowledge

Thank you

David Porter

Resilient Thinking

david.porter@resilientthinking.co.uk
www.resilientthinking.co.uk