Lessons From The Legion

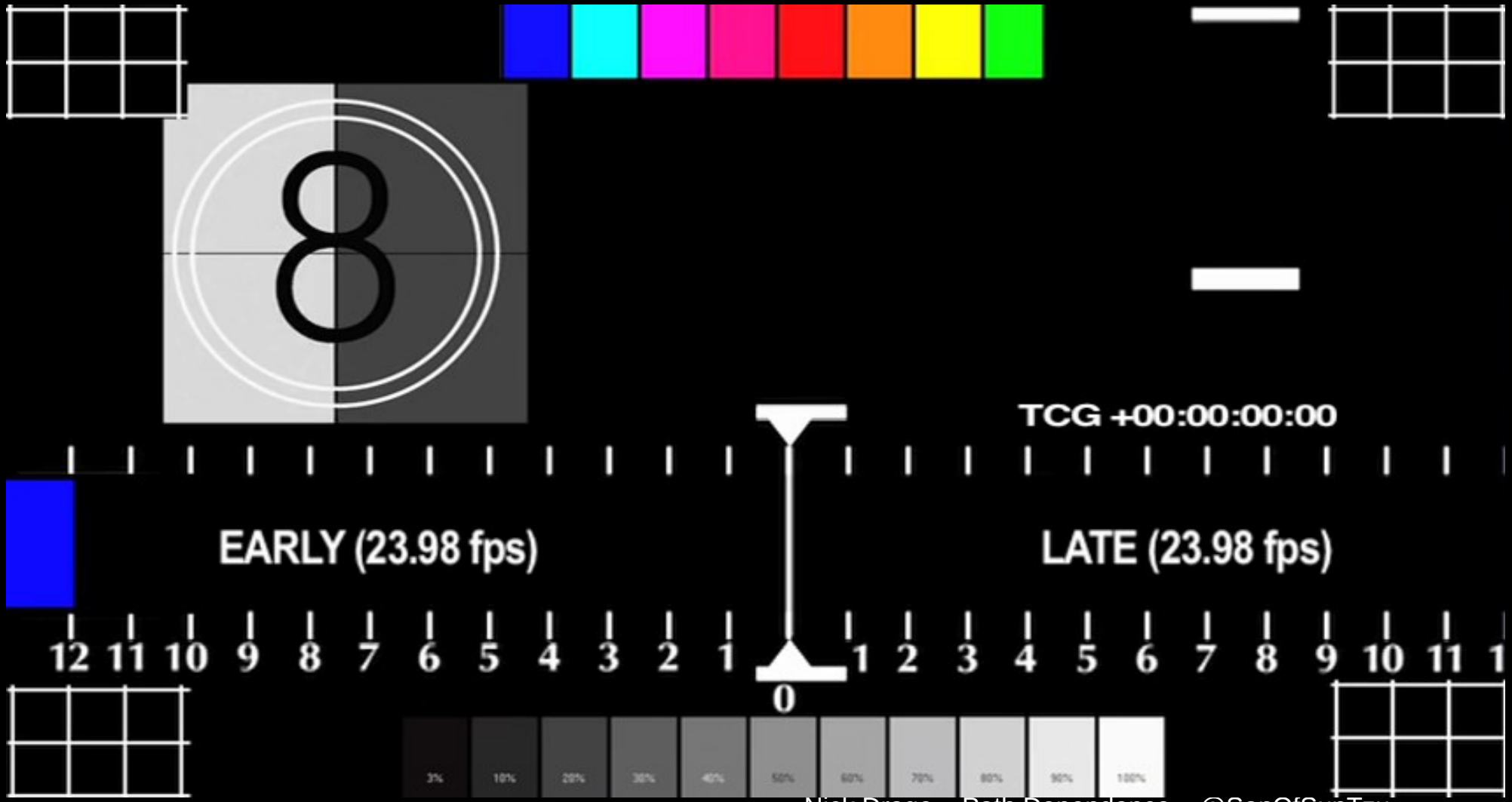
Nick Drage
Path Dependence Limited

October CyberTech - 18 Oct 2018

V 4.7

Testing, testing, 1 2 3

- Plugged in?
- Are you at the Huckletree?
- Water?
- Audio and video...


8
TCG +00:00:00:00
EARLY (23.98 fps)
LATE (23.98 fps)
12 11 10 9 8 7 6 5 4 3 2 1 0 1 2 3 4 5 6 7 8 9 10 11 1
3%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Lessons From The Legion

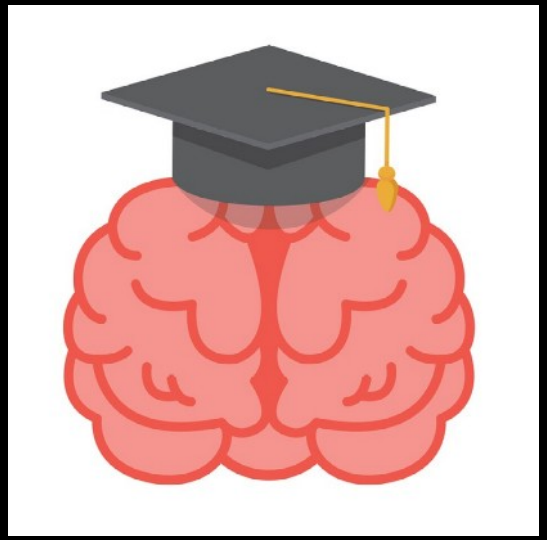
Nick Drage

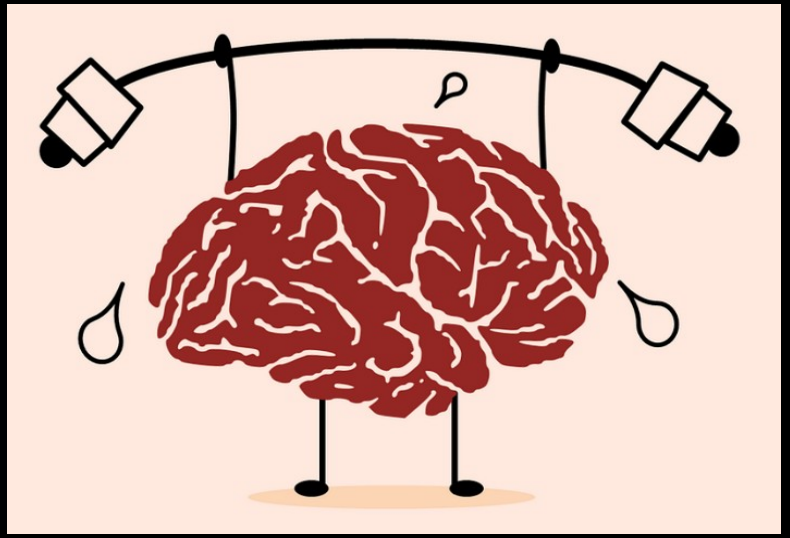
“London CyberTech Remix”

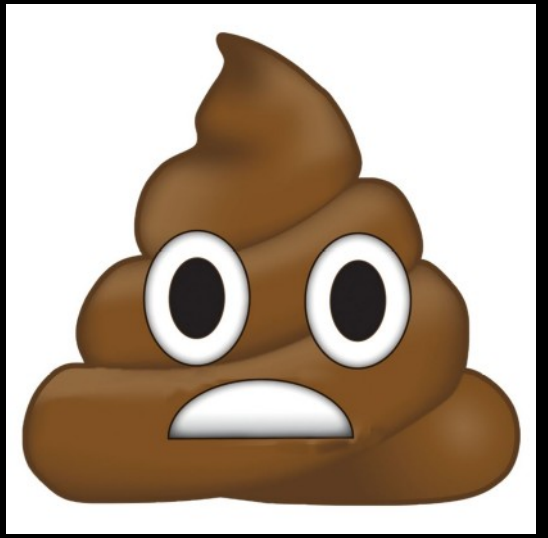
October CyberTech - 18 Oct

twitter.com/ch33r10

I have a question, not a solution







You'll Have Questions...

- Here all evening
- Contact details at the end
- All references blogged
- All media – owner's copyright
- If no credit, probably Pixabay

Nick Drage – Path Dependence – @SonOfSunTzu

Win the Cyberwar With Zero Trust

John Kindervag

Field CTO

The Four Levels of War

Grand Strategy (Political)	The Ultimate Goal
Strategy	The Big Idea
Tactics	The Things You Use
Operations	The Way You Use Them

The Four Levels of Cyberwar

Grand Strategy (Political)	Stop Data Breaches
Strategy	Zero Trust
Tactics	Tools/Policies
Operations	Platform

The Four Levels of Cyberwar

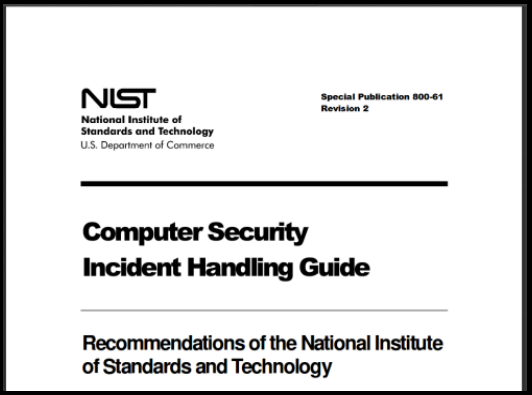
Grand Strategy (Political)	The Ultimate Goal
Strategy	The Big Idea
Tactics	The Things You Use
Operations	The Way You Use Them

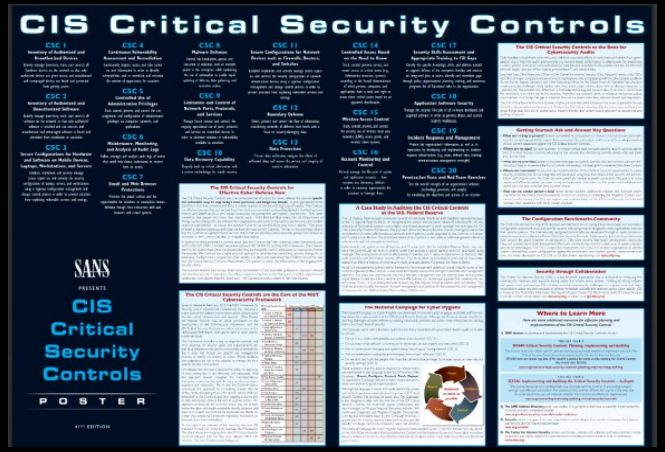
Tactics

- System Administrators / Developers
- Penetration Testers
- Incident Responders

“The Big Idea”

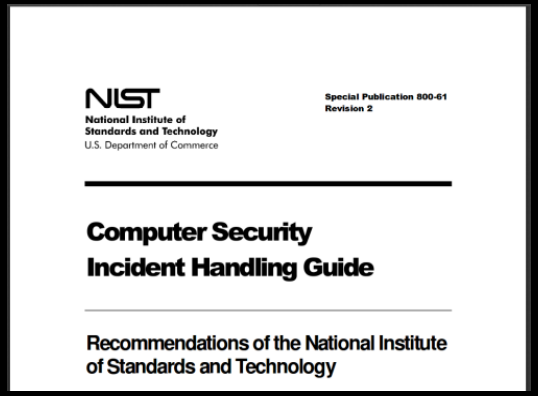
- System Administrators / Developers
- Penetration Testers
- Incident Responders





“The Big Idea”

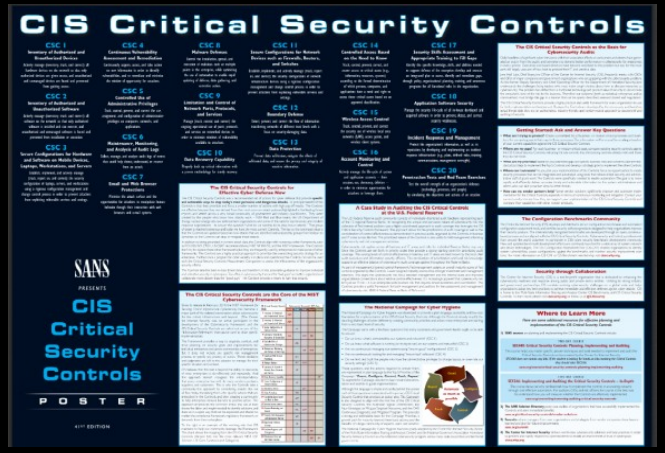
- System Administrators / Developers
  - Harden my stuff
- Penetration Testers
  - Continual technical improvement
- Incident Responders
  - Playbooks ready


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

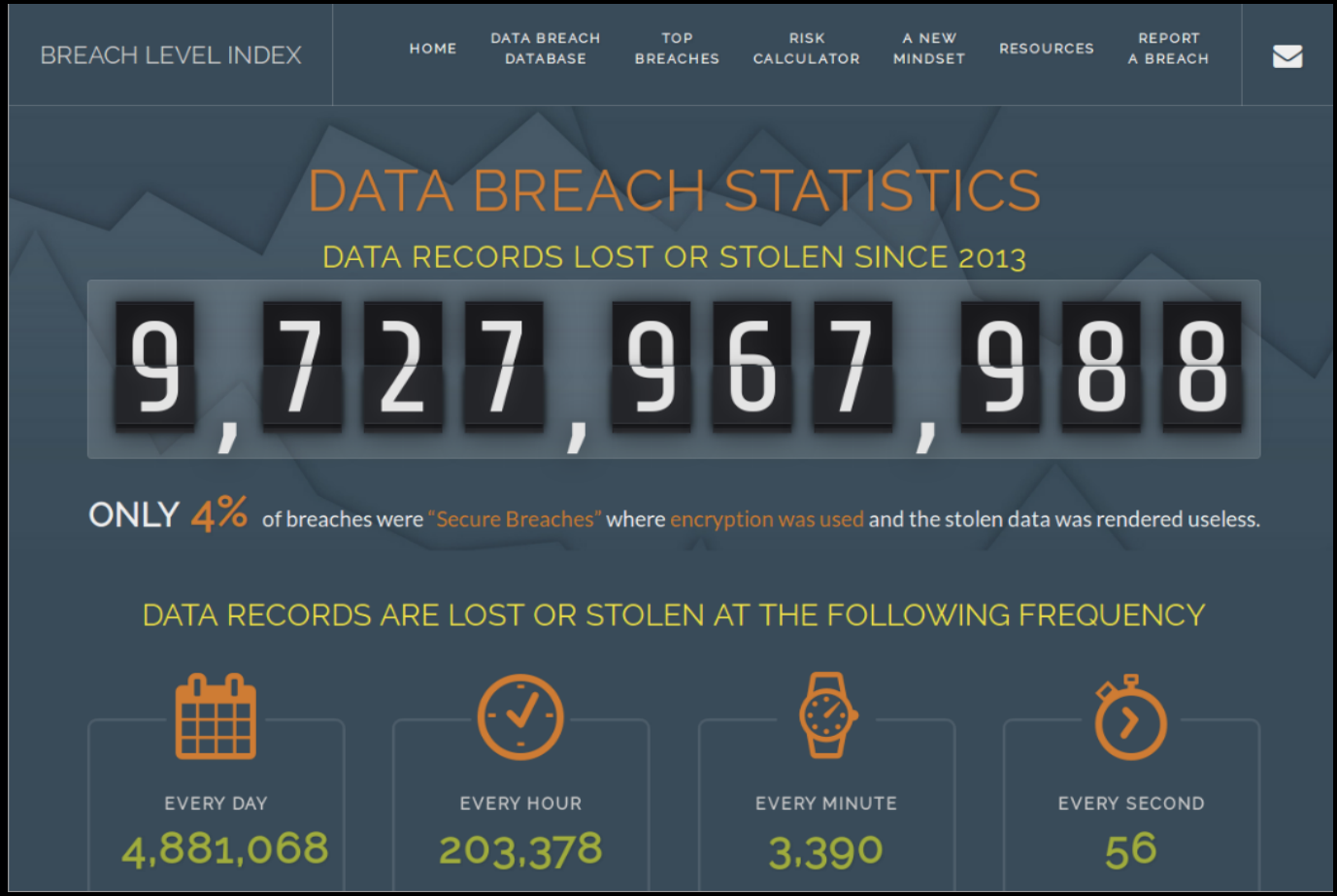
Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

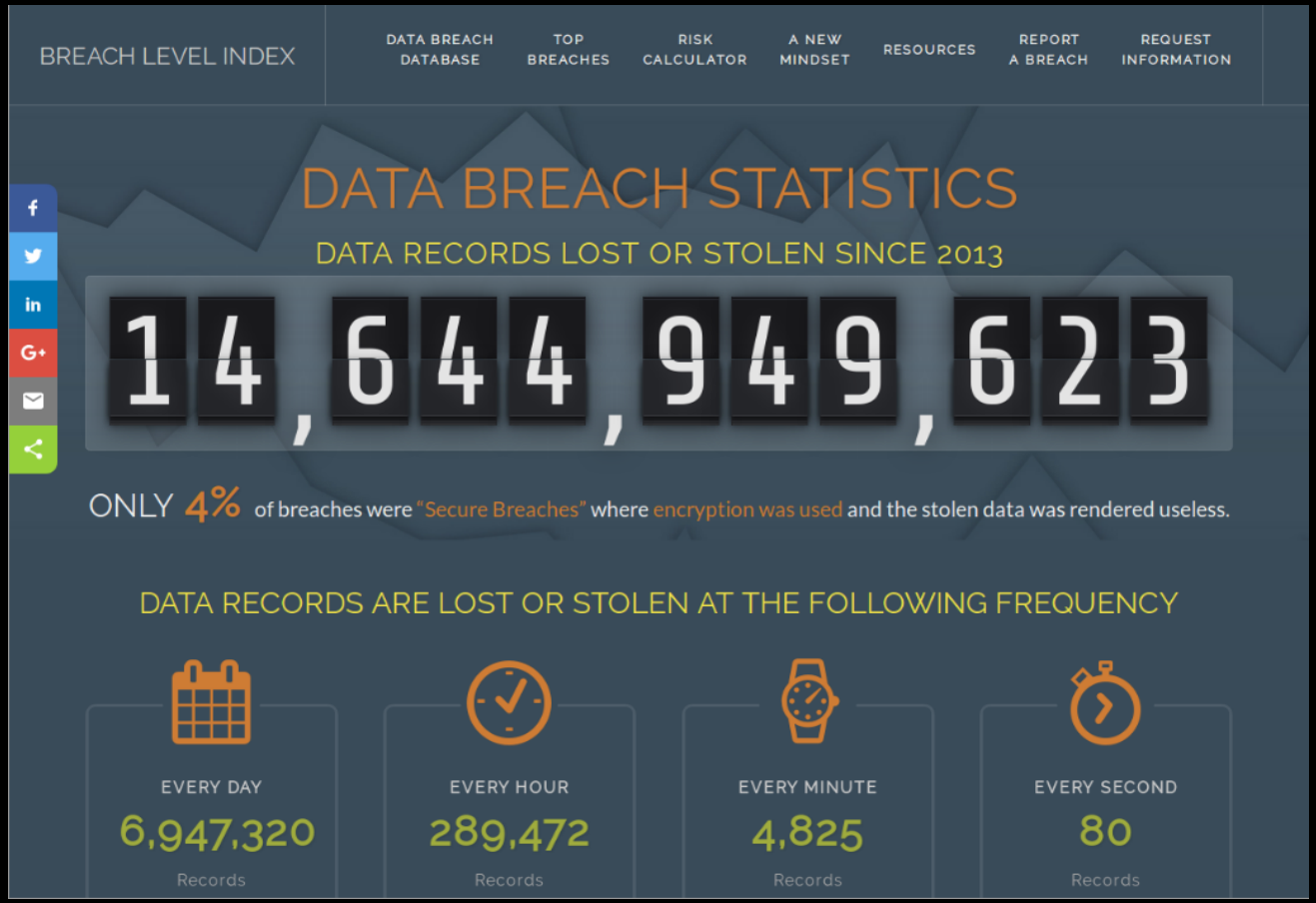


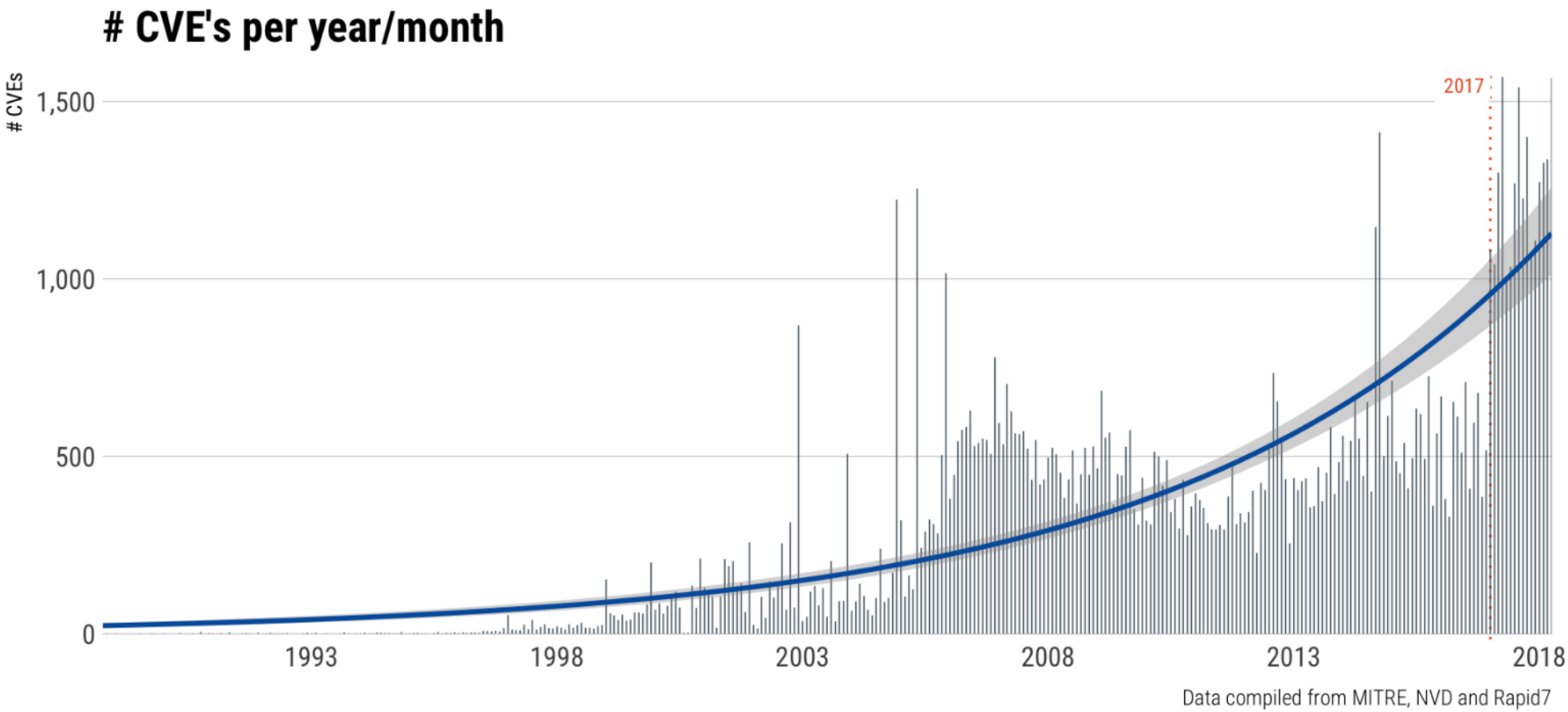
How do we learn and train

BreachLevelIndex.com



BreachLevelIndex.com




CVE's per year/month
CVEs
1,500
1,000
500
0
2017
1993
1998
2003
2008
2013
2018
Data compiled from MITRE, NVD and Rapid7

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

The Global Risks Report 2018

13th Edition

Figure I: The Global Risks Landscape 2018

The Four Levels of Cyberwar

- Grand Strategy (Political)
- **Strategy**
- Tactics
- Operations

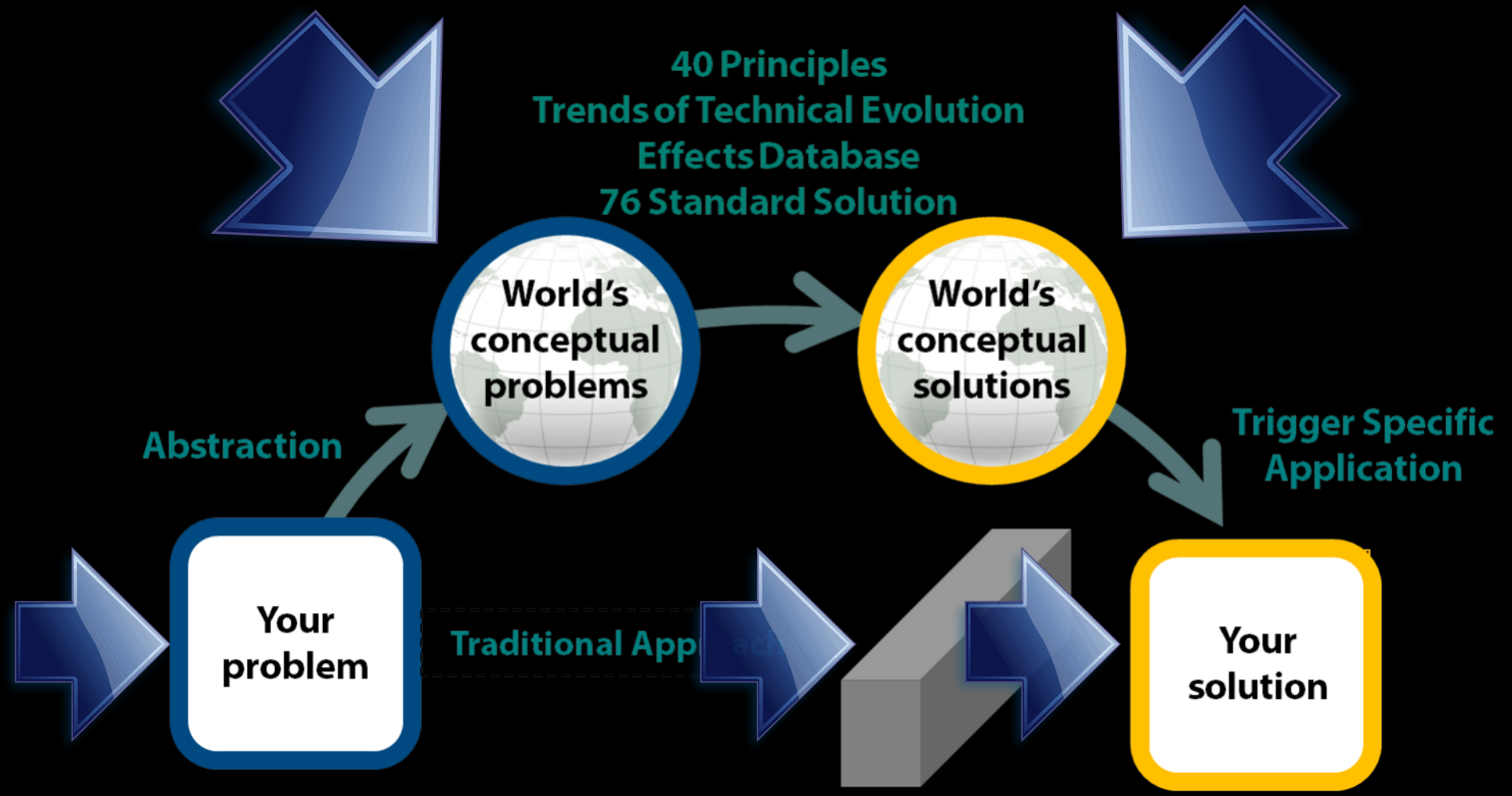
Image: Costume Supe

Nick Drage – Path Dependence – @SonOfSunTzu

https://www.competitivedge.com/catalog/all-sports

TRIZ

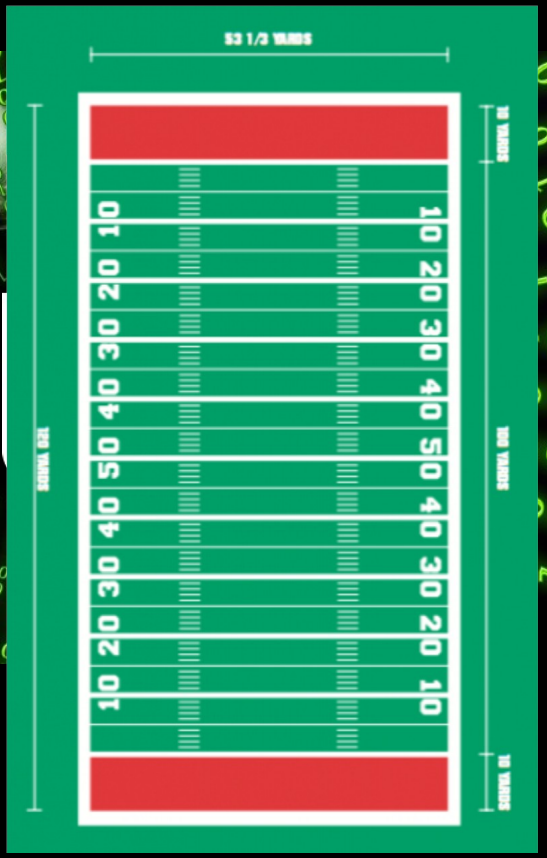
- Russian - “Theory of Inventive Problem Solving”
- Characteristics of problems
- Patterns in solutions
- A sufficient level of abstraction
- Use other’s solutions



So ...


42

- Utterly incomprehensible from outside
- Complex
- Team games
- Highly specialised
  - By situation
  - Attack or Defend
- Fight over territory
- Offensive or defensive playbooks



https://media.defense.gov/


Region Overflow
Region Overflow
USARNORTH


3RD & 10
NFL.com Fantasy Touchdown
Lazzy Fitzgerald Highlight Available
Press to view
Screens simulated; subject to change.
XBOX

SEATTLE SEAHAWKS

Offense	Starter	2nd String	3rd String
QB	Russell Wilson	**Tarvaris Jackson**	Terrelle Pryor
HB	Marshawn Lynch	Robert Turbin	
HB2	Christine Michael		
FB	Derrick Coleman	Spencer Ware	Kiero Small
TE-Y	Zach Miller	Anthony McCoy	
TE-H	Luke Willson		
WR1	Percy Harvin	Paul Richardson	Bryan Waters
WR2	Doug Baldwin	Sidney Rice	Ricardo Lockette
SWR	Jermaine Kearse	Kevin Norwood	
LT	Russell Okung	Alvin Bailey	
LG	James Carpenter	Caylin Hauptmann	
C	Max Unger	Lemuel Jeanpierre	Greg Van Roten
RG	J.R. Sweezy	Steve Schilling	
RT	Michael Bowie	Justin Britt	

Defense	Starter	2nd String	3rd String
DLE	Michael Bennett	Greg Scruggs	Benson Mayowa
DLT	Tony McDaniel	**Kevin Williams**	Jordan Hill/D'Anthony Smith
DRT	Brandon Mebane	Jesse Williams	Jimmy Staten
DRE	Cliff Avril	Cassius Marsh	O'Brien Schofield
SLB	Bruce Irvin	Malcolm Smith	
MLB	Bobby Wagner	**Heath Farwell**	
WLB	K.J. Wright	Michael Morgan	Kevin Pierre-Louis
LCB	Richard Sherman	Tharold Simon	AJ Jefferson
RCB	Byron Maxwell	Phillip Adams	Eric Pinkins
SCB	Jeremy Lane	DeShawn Shead	
SS	Kam Chancellor	Jeron Johnson	
FS	Earl Thomas		

Special Teams	Starter	2nd String	
K	Steven Hauschka		
P	**Jon Ryan**		
LSN	Clint Gresham		

THE LEGION OF

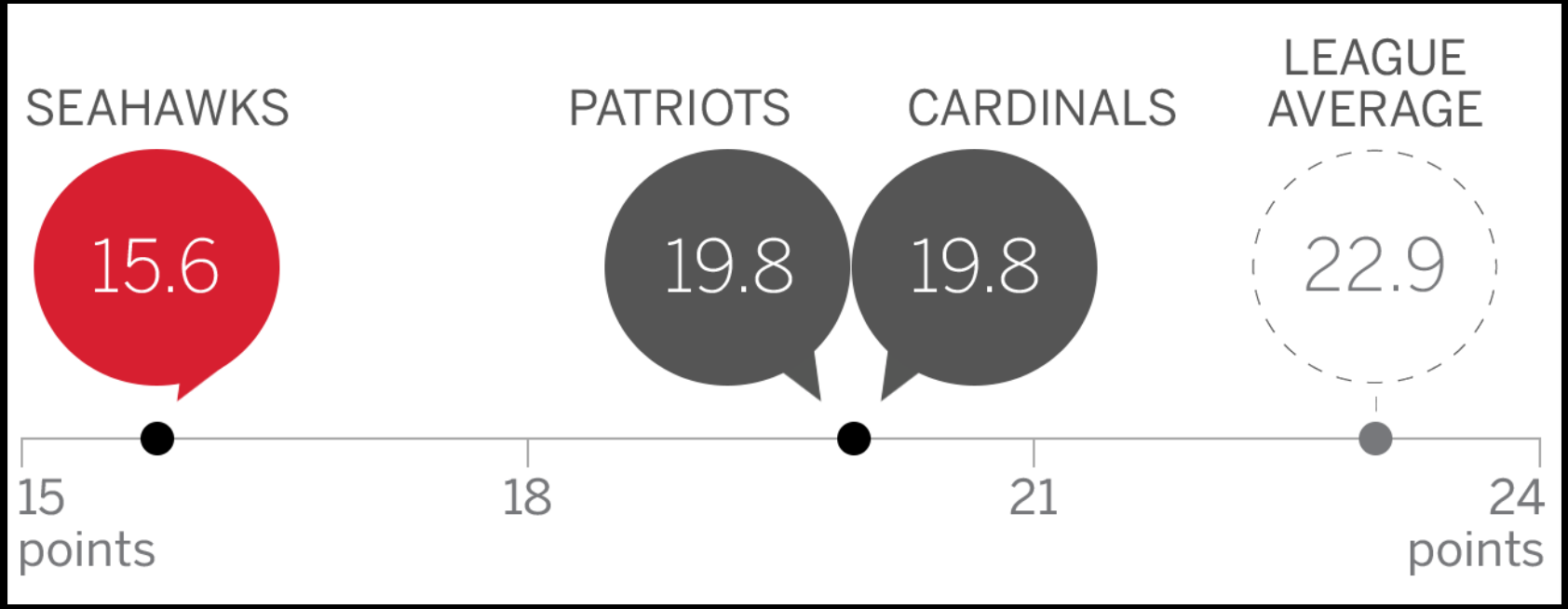
BOOM

Seattle Seahawks' Defense – 2011 to 2017

- Sherman - CornerBack
- Thomas – Free Safety
- Chancellor – Strong Safety
- Everyone

2012-2015

- Fewest points allowed 2012, 2013, 2014, 2015 – NFL Record



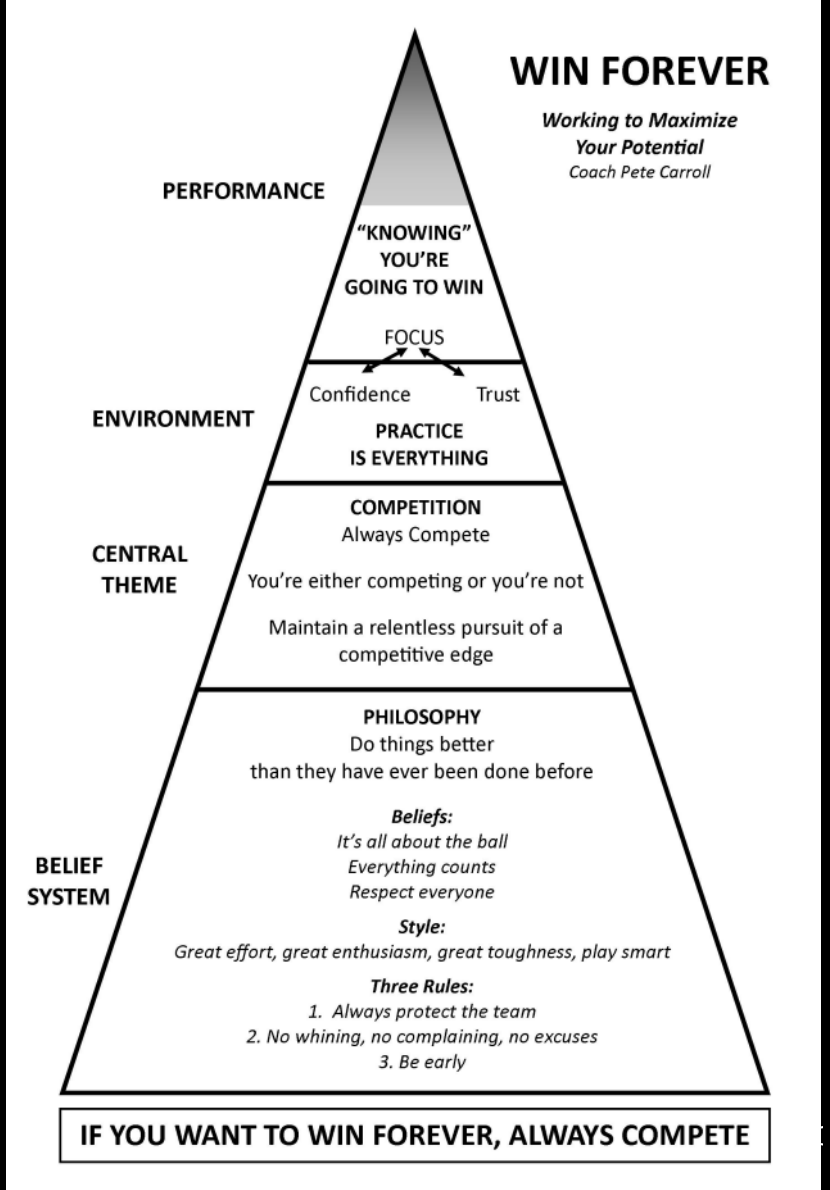
ESPN

2012-2015

- Lead the league – Fewest Passing Yards Allowed
- Lead the league – Fewest First Downs
- 2nd Quarterback Pressures
- 4th Rushing Yards per carry
- 6th in takeways
- Always high in DVOA ranking

LESSON – Train how you fight

Practice is everything




SUPER BOWL CHAMPIONS
SUPER BOWL XLVIII
MetLife
SUPER BOWL XLVIII

SEAHAWKS

Offense	Starter	2nd String	3rd String
QB	Russell Wilson	[illegible]son	Terrelle Pryor
HB	Marshawn Lynch	[illegible]rbin	
HB2	Christine Michael		
FB	Derrick Coleman	Spencer Ware	Kiero Small
TE-Y	Zach Miller	Anthony McCoy	
TE-H	[illegible] Willson		
WR1	[illegible]y Harvin	Paul Richardson	Bryan Waters
WR2	[illegible]aldwin	Sidney Rice	Ricardo Lockette
SWR	[illegible]earse	Kevin Norwood	
LT	Russel[illegible]g	Alvin Bailey	
LG	James Carp[illegible]	Cayli[illegible]auptmann	
C	Max Unger	Le[illegible]el Jeanpierre	Greg Van Roten
RG	J.R. Sweezy	Steve Schilling	
RT	Michael Bowie	Justin Britt	

Defense	Starter	2nd String	3rd String
DLE	Michael Benn[illegible]	[illegible]eg Scruggs	Benson Mayowa
DLT	Tony McD[illegible]	**Kev[illegible] Williams**	Jordan Hill/D'Anthony Smith
DRT	Brandon[illegible]ane	Jesse [illegible]illiams	Jimmy Staten
DRE	C[illegible]ril	Cassius M[illegible]rsh	O'Brien Schofield
SLB	[illegible] Irvin	Malcolm Smi[illegible]	
MLB	[illegible] Wagner	**Heath Farwell**	
WLB	K.J. Wright	Michael Morgan	Kevin Pierre-Louis
LCB	Richard Sherman	Tharold Simon	AJ Jefferson
RCB	Byron Maxwell	Phillip Adams	Eric Pinkins
SCB	Jeremy Lane	DeShawn Shead	
SS	Kam Chancellor	Jeron Johnson	
FS	Earl Thomas		

Special Teams	Starter	2nd String	
K	Steven Hauschka		
P	**Jon Ryan**		
LSN	Clint Gresham		

The Caffrey Triangle

Rory McCune - Penetration Testing Must Die

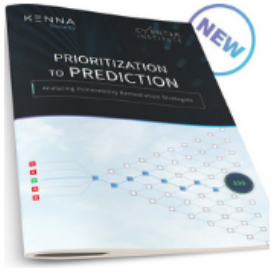
441 views

Jeremiah Grossman

@jeremiahg

Follow

"Less than 2% of vulnerabilities are actively exploited in the wild, making traditional remediation very inefficient, costly, and time-consuming."



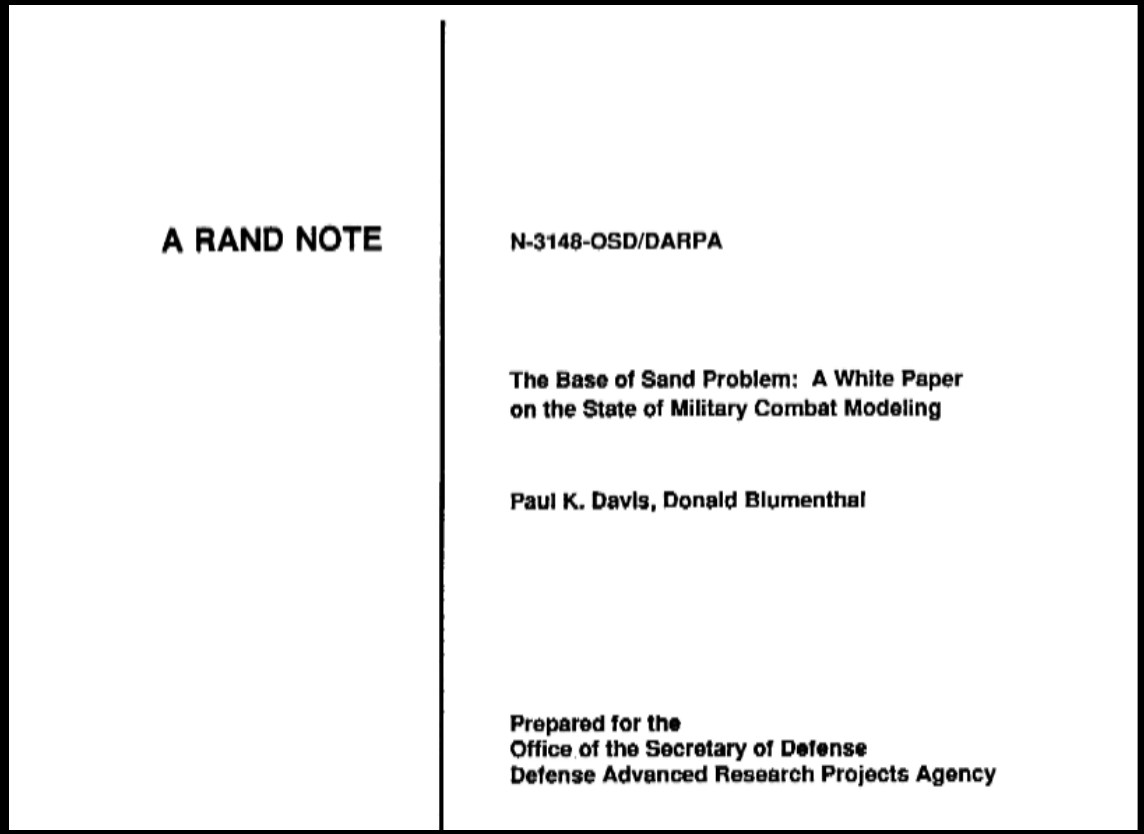
Kenna Security @KennaSecurity

Have you heard about our report with @cyentiainst this morning? It provides a quantitative look at the effectiveness of common remediation strategies. See the full report here: bit.ly/2IGrlG0

12:18 pm - 15 May 2018

Common traps & pitfalls in red-teaming Andrew Davies & Jon Medvenics, Netscylla

The Base of Sand Problem



A RAND NOTE

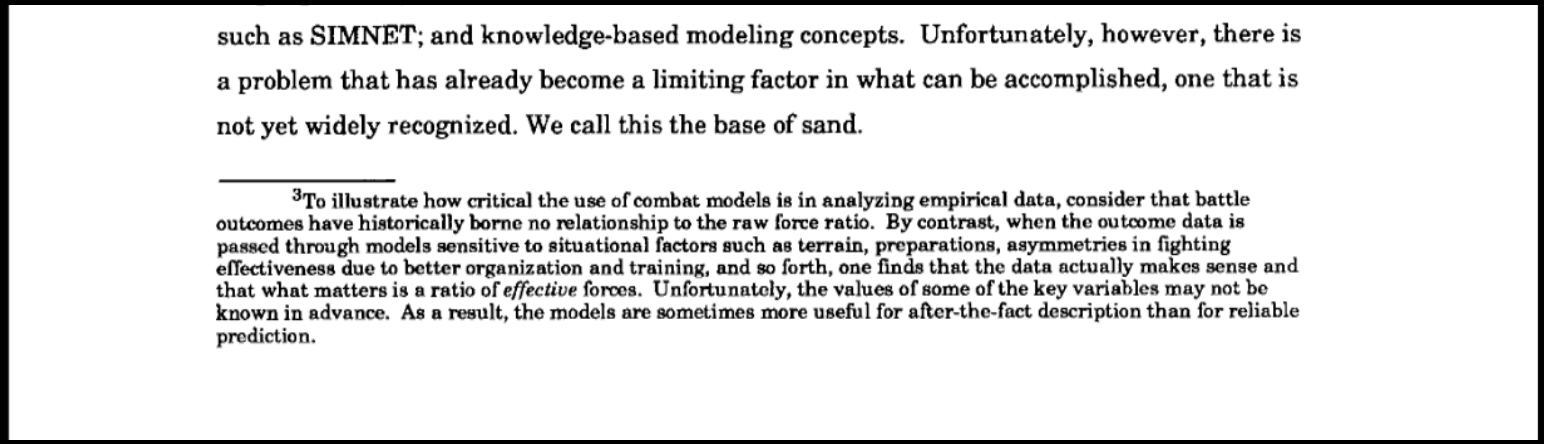
N-3148-OSD/DARPA

The Base of Sand Problem: A White Paper on the State of Military Combat Modeling

Paul K. Davis, Donald Blumenthal

Prepared for the
Office of the Secretary of Defense
Defense Advanced Research Projects Agency

Footnote 3



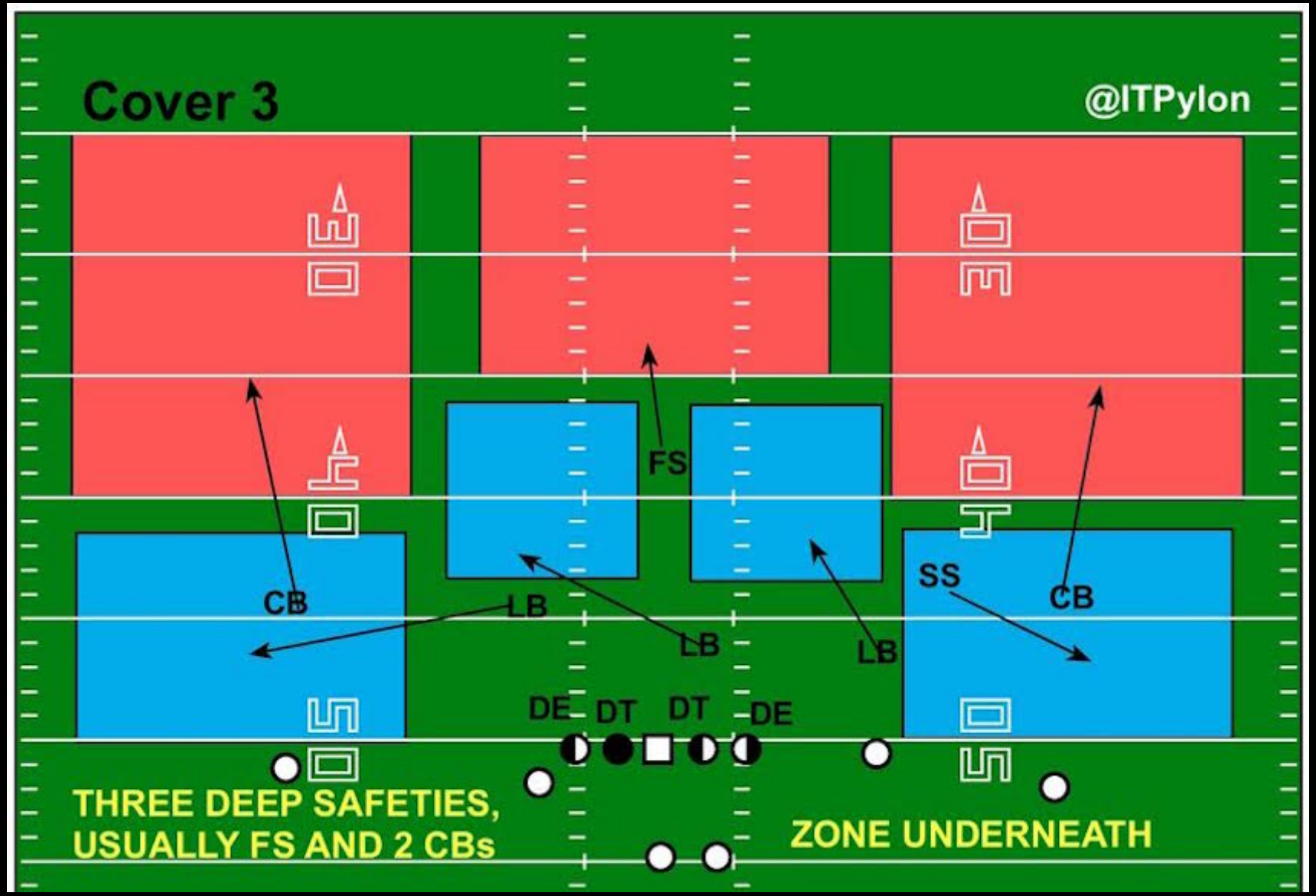
such as SIMNET; and knowledge-based modeling concepts. Unfortunately, however, there is a problem that has already become a limiting factor in what can be accomplished, one that is not yet widely recognized. We call this the base of sand.

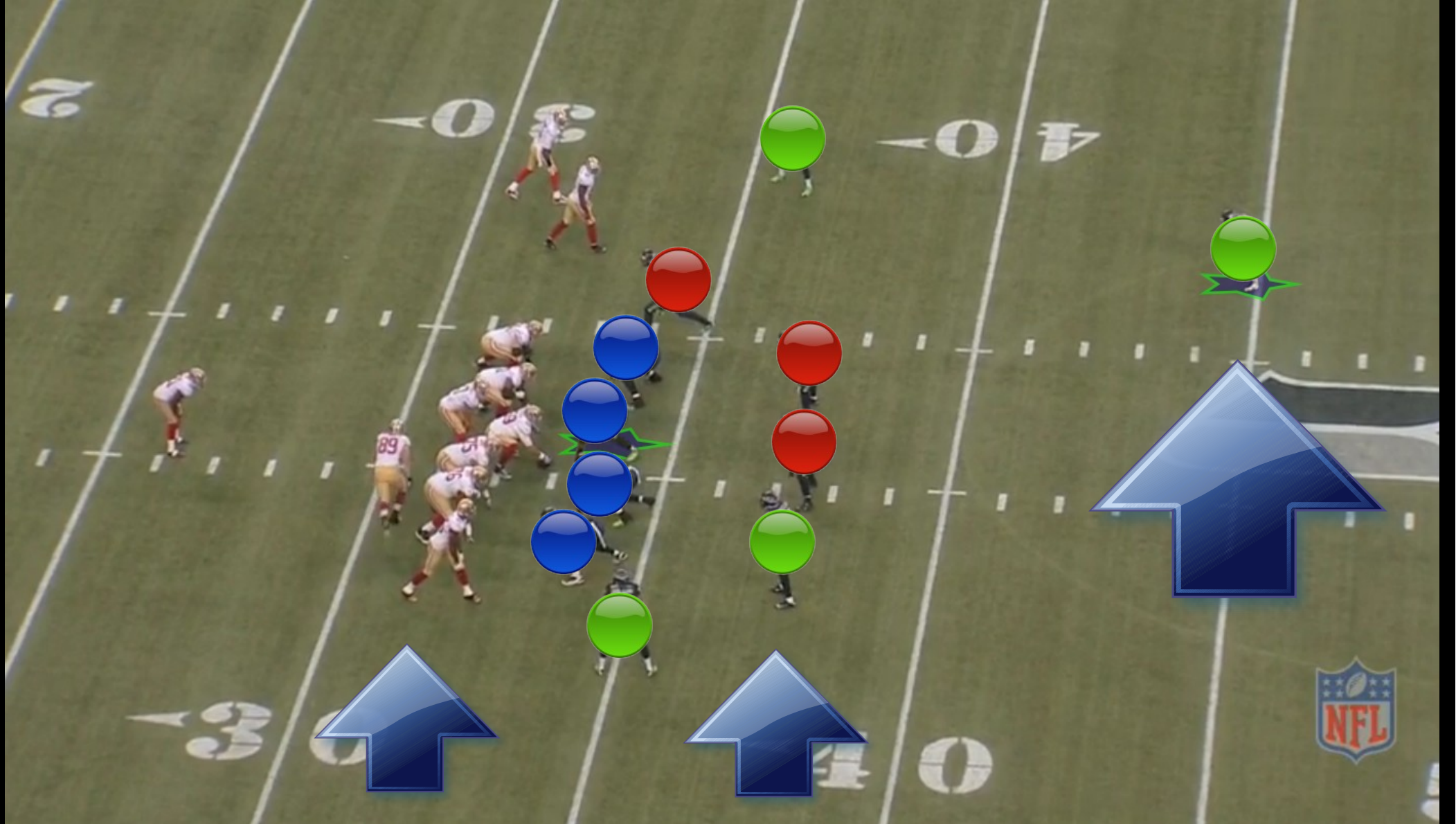
[3]To illustrate how critical the use of combat models is in analyzing empirical data, consider that battle outcomes have historically borne no relationship to the raw force ratio. By contrast, when the outcome data is passed through models sensitive to situational factors such as terrain, preparations, asymmetries in fighting effectiveness due to better organization and training, and so forth, one finds that the data actually makes sense and that what matters is a ratio of *effective* forces. Unfortunately, the values of some of the key variables may not be known in advance. As a result, the models are sometimes more useful for after-the-fact description than for reliable prediction.

“Battle outcomes have historically borne no relationship to the raw force ratio...

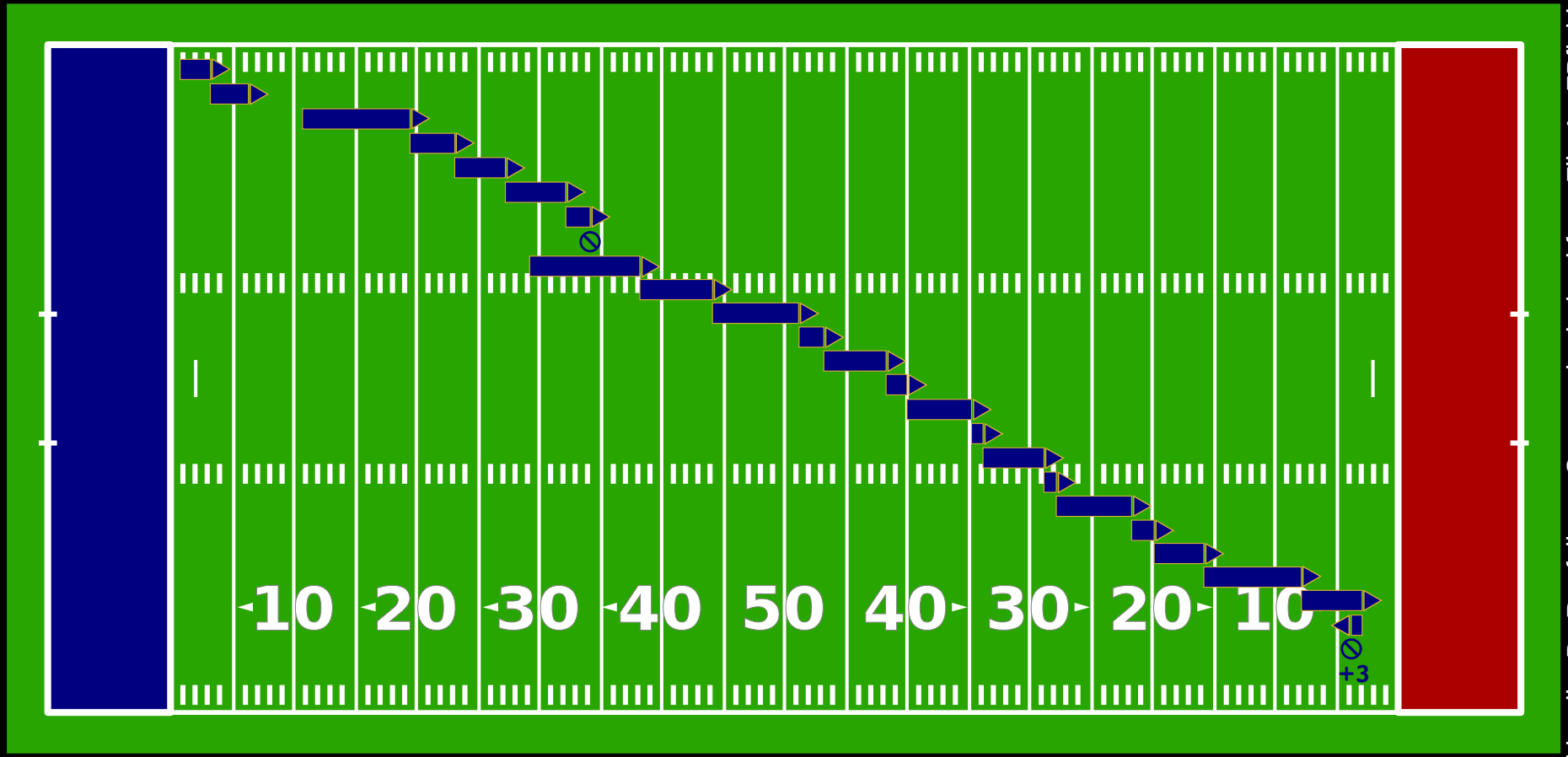
...what matters is the ratio of *effective* forces” (emphasis mine)

LESSON – Eliminate the big play


Cover 3
@ITPylon
30
30
30
FS
CB
LB
LB
LB
SS
CB
DE
DT
DT
DE
THREE DEEP SAFETIES,
USUALLY FS AND 2 CBs
ZONE UNDERNEATH


NFL

Drive chart



How breaches work (percep

Getting hacked (common perception)

1. Attacker's Exploit Succeeds

How breaches work (perception vs reality)

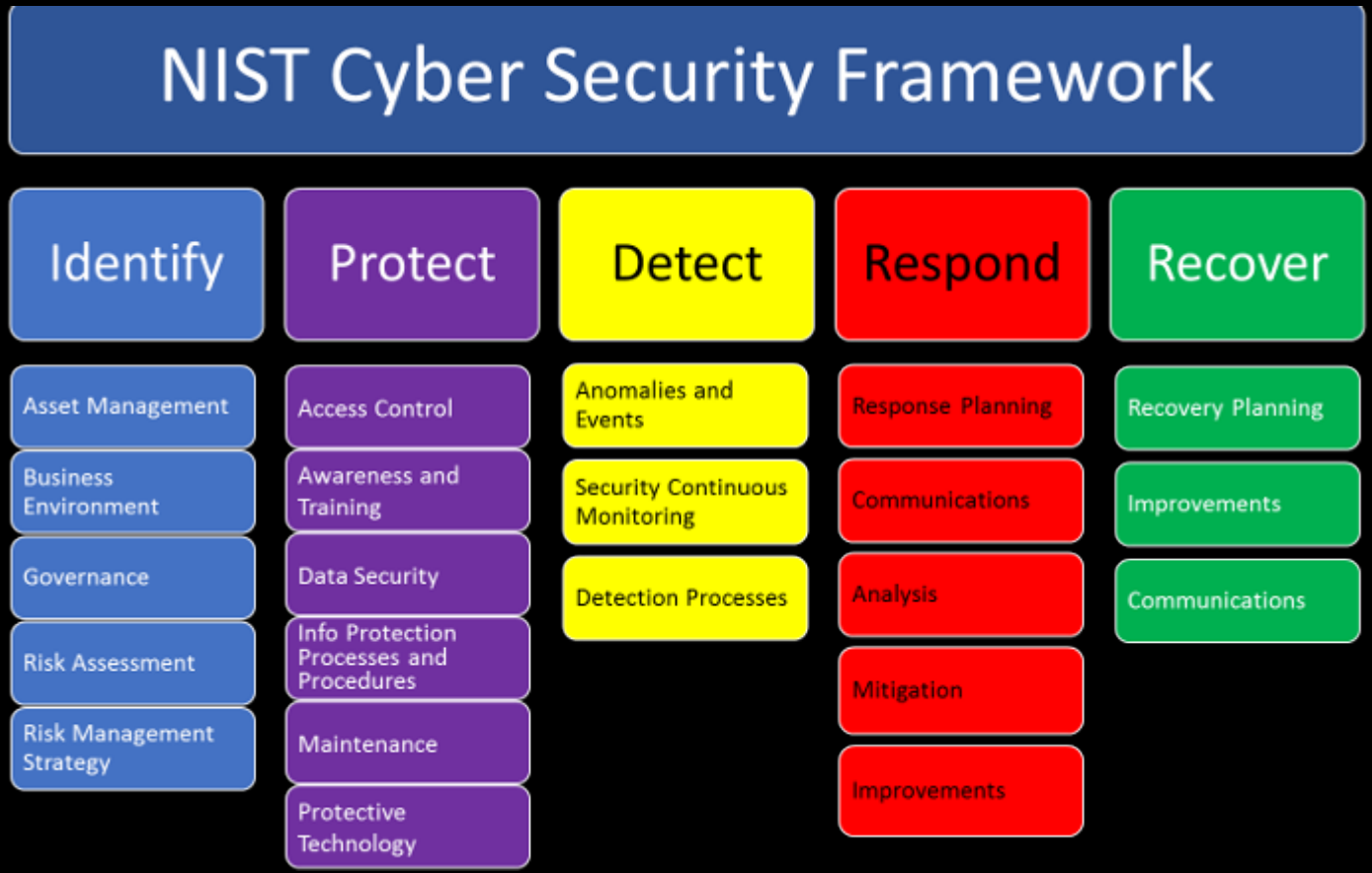
Getting hacked (common perception)

1. Attacker's Exploit Succeeds

Reality

1. Exploit succeeds
2. Escalate privileges
3. Scans network
4. Dumps/cracks creds
5. Pivots
6. Creates additional accounts
7. Exfiltrates data

NIST – five core functions



Nick Drage – Path Dependence – @SonOfSunTzu

https://medium.com/@TechTieu/cyber-security-framework-66aa07c1b7a5

NIST – five core functions

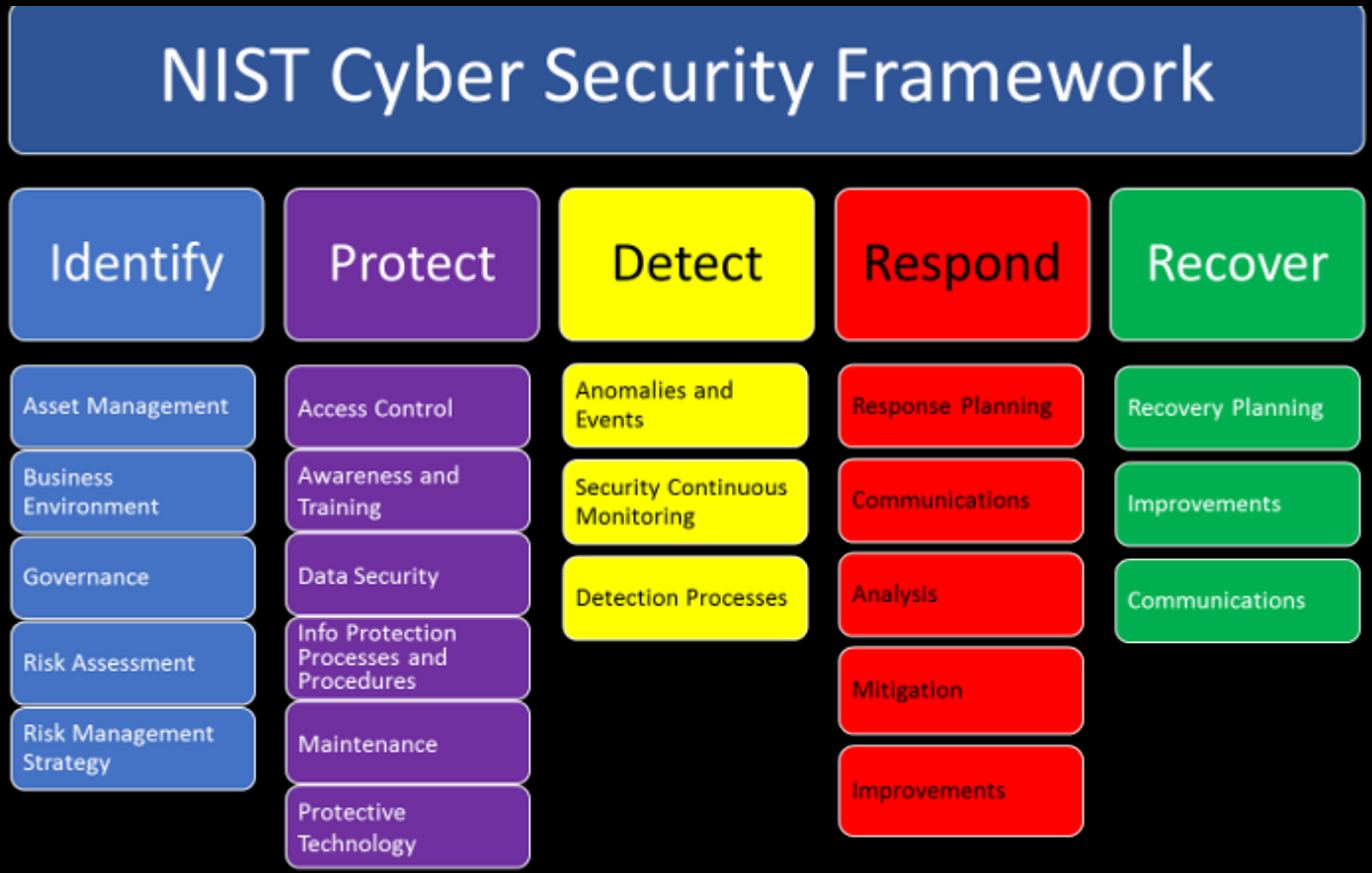
https://medium.com/@TechTieu/cyber-security-framework-66aa07c1b7a5

NIST – five core functions

Nick Drage – Path Dependence – @SonOfSunTzu

https://medium.com/@TechTieu/cyber-security-framework-66aa07c1b7a5

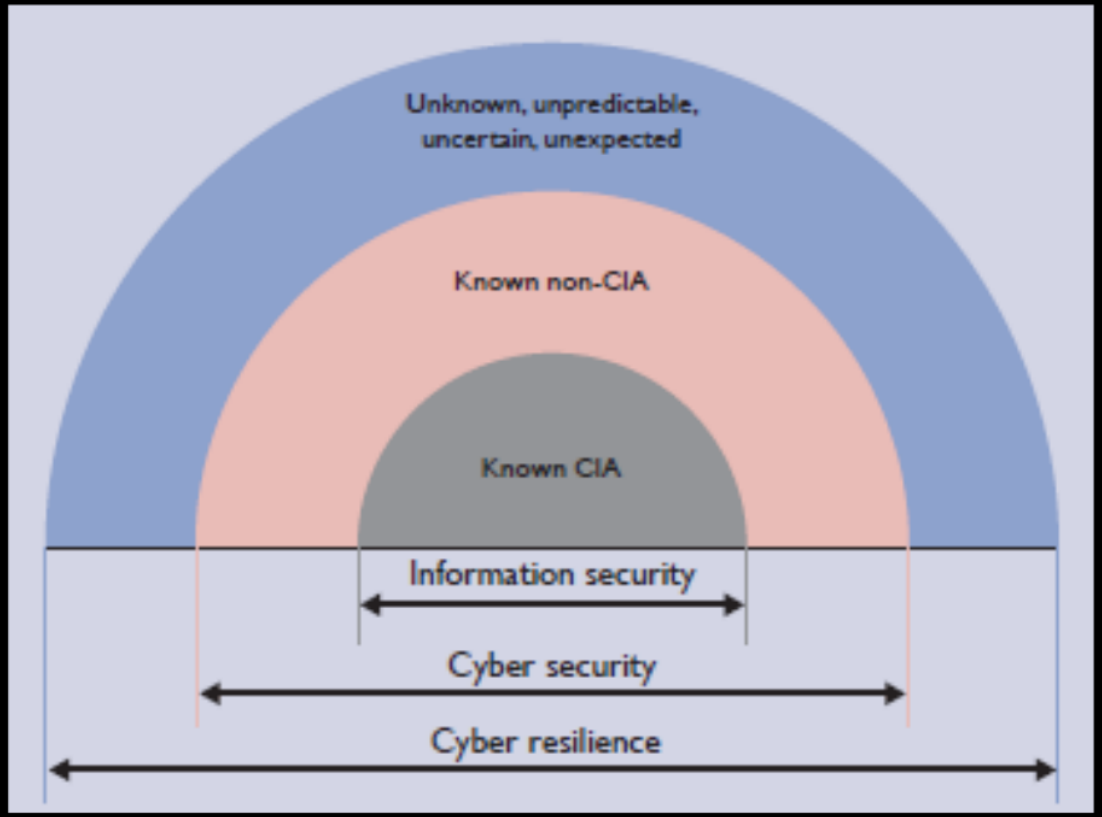
NIST – five core functions



Nick Drage – Path Dependence – @SonOfSunTzu

https://medium.com/@TechTieu/cyber-security-framework-66aa07c1b7a5

As we're meant to be resilient now

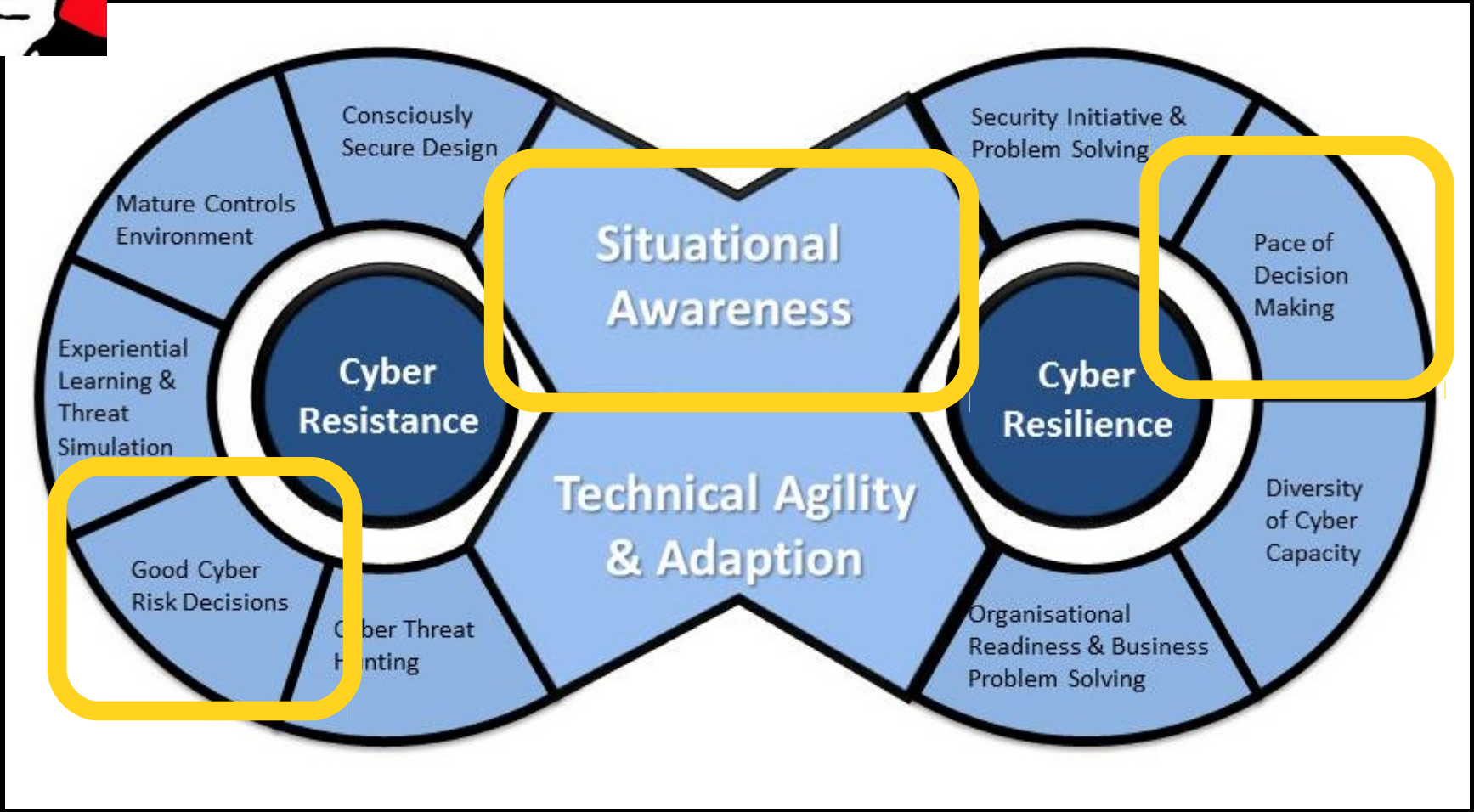


Source: ISF - Cyber Security Strategies

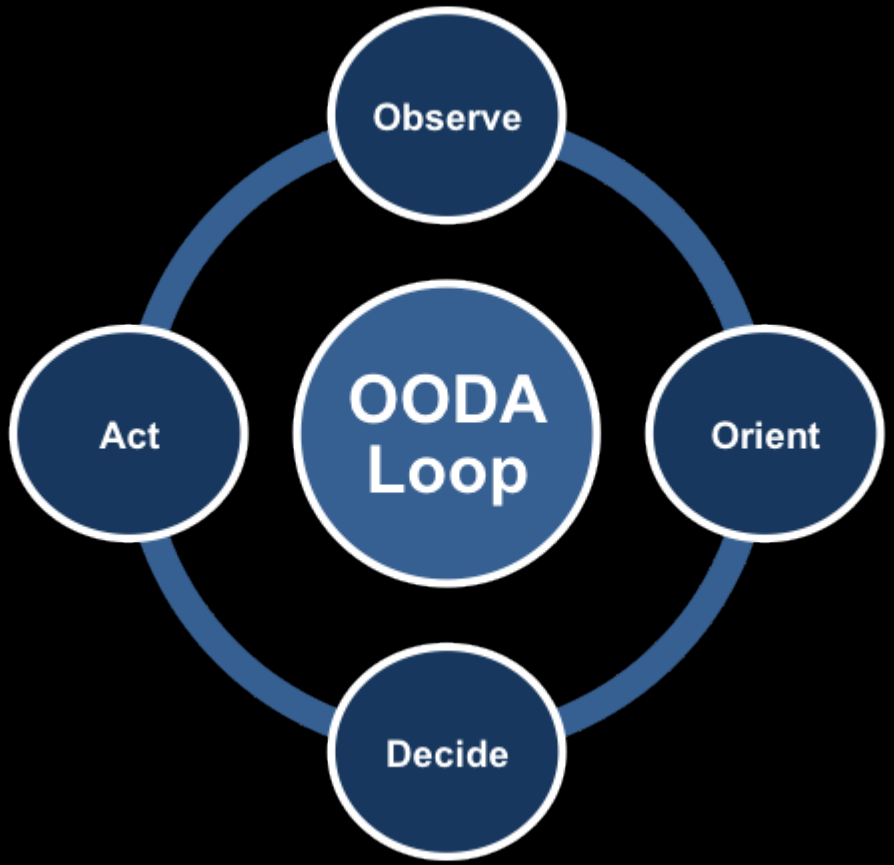
Symantec.

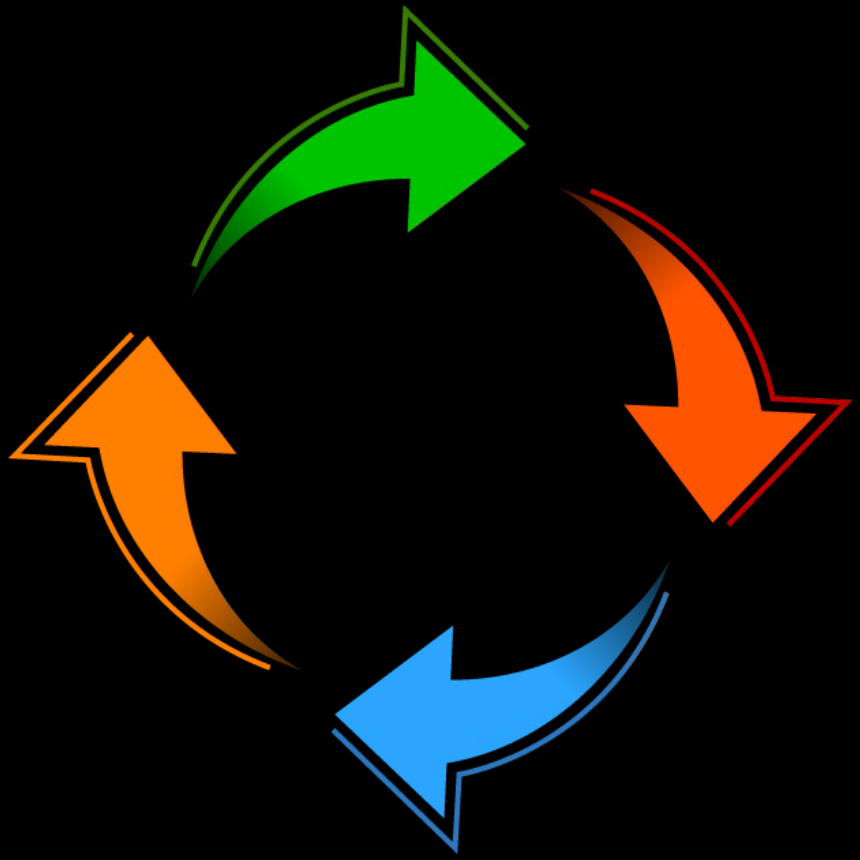
http://csd.ncb.mu/English/Pages/Presentations/Mauritius%20Event%20Dec2013v1%20Symantec.pdf

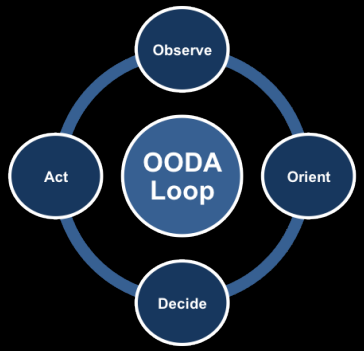
Blog - Black Swan Security

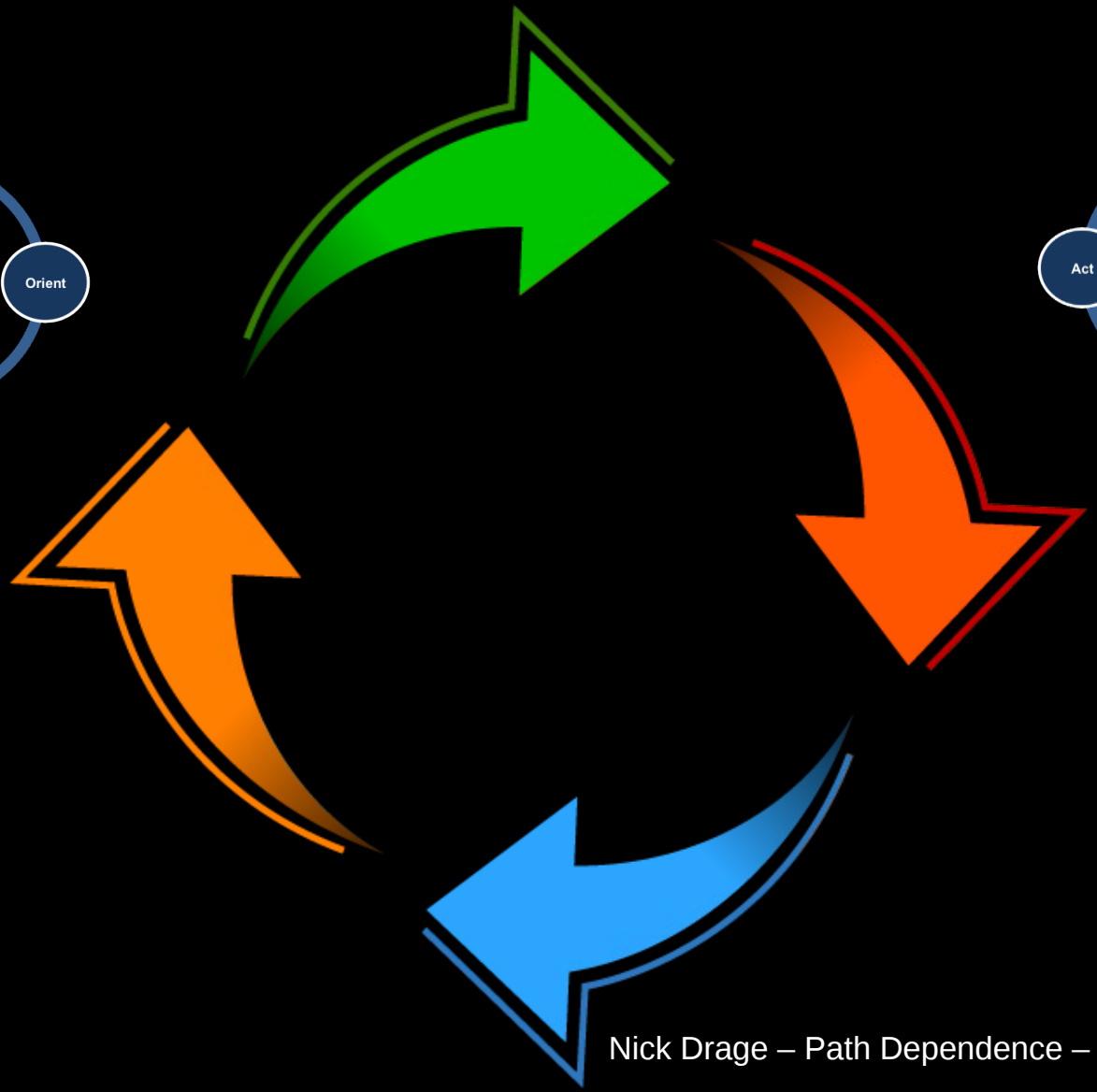


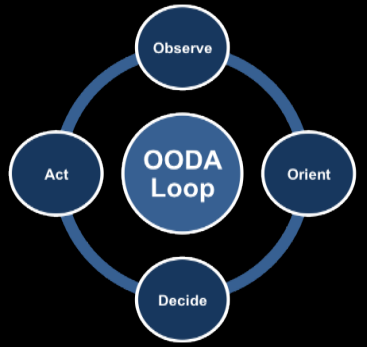
OODA: Observe – Orient – Decide - Act



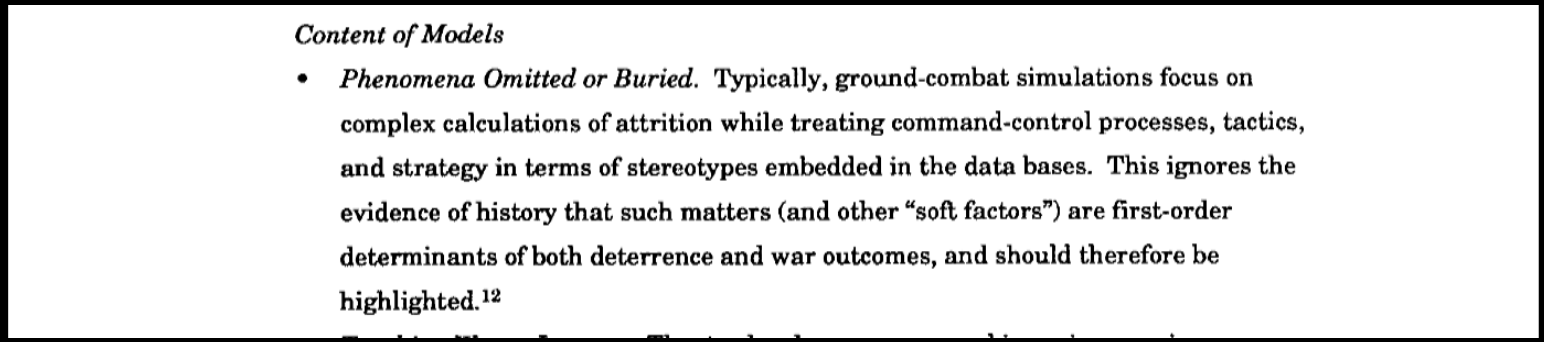



Observe
Act
OODA Loop
Orient
Decide




Observe
Act
OODA Loop
Orient
Decide

LESSON – out hit your opponent



Content of Models

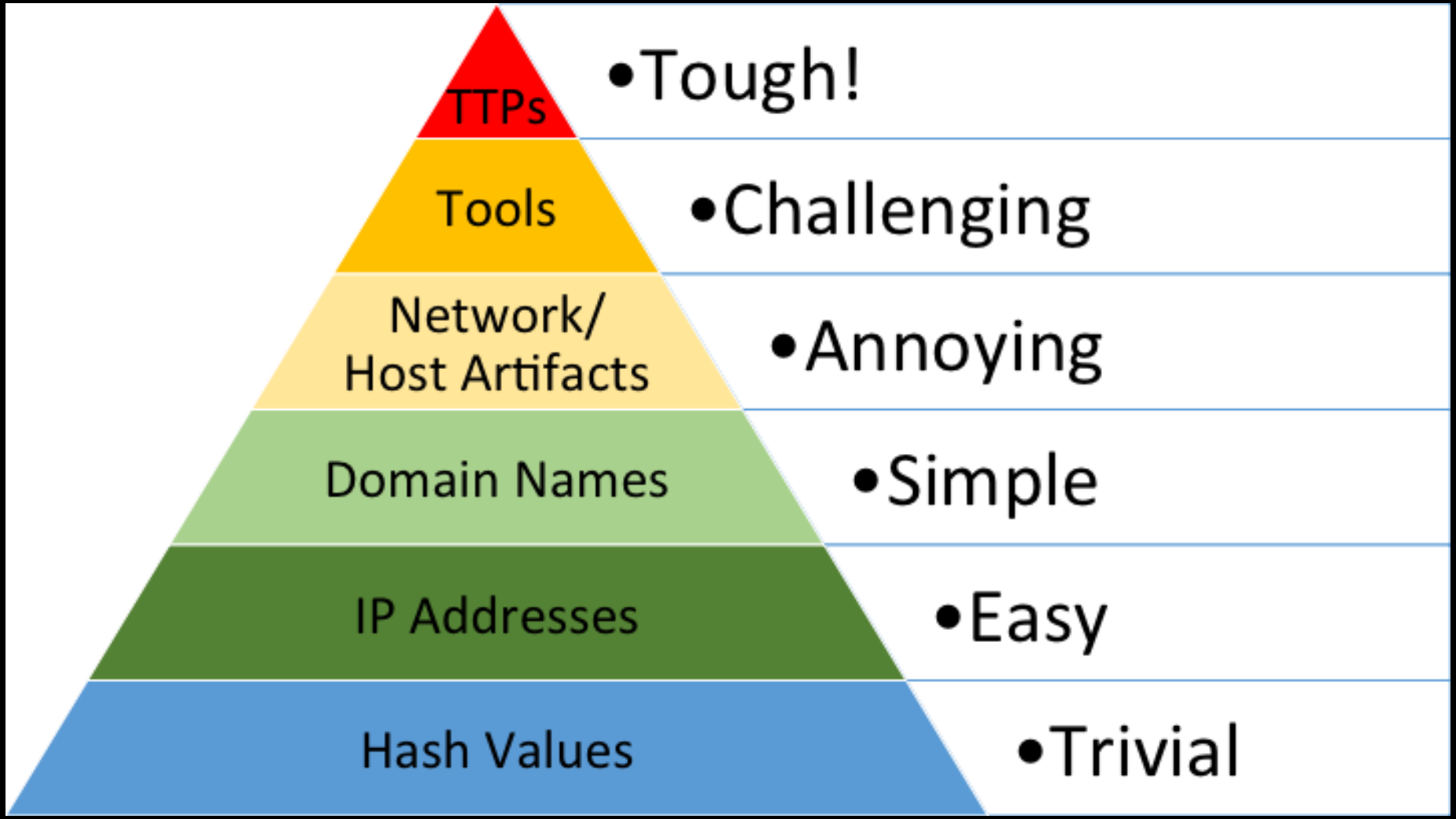
- *Phenomena Omitted or Buried.* Typically, ground-combat simulations focus on complex calculations of attrition while treating command-control processes, tactics, and strategy in terms of stereotypes embedded in the data bases. This ignores the evidence of history that such matters (and other "soft factors") are first-order determinants of both deterrence and war outcomes, and should therefore be highlighted.[12]

The evidence of history is that soft factors: command-control processes, tactics, and strategy, are *first-order determinants* of both deterrence and war outcomes (emphasis mine)

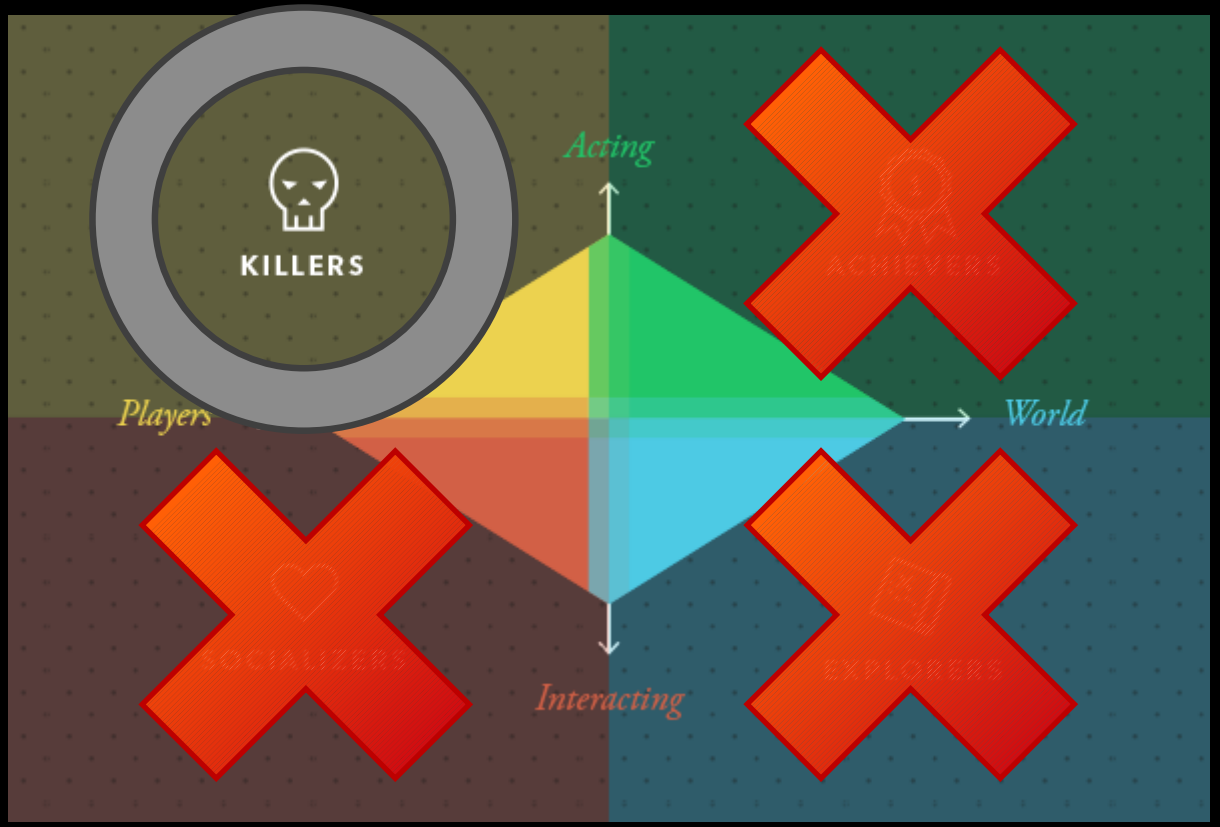
THE LEGION OF

BOOM


RICHARD SHERMAN
"HE'S A FREAKING MONSTER. HE DAMAGES PEOPLE'S SOULS."


TTPs
•Tough!
Tools
•Challenging
Network/
Host Artifacts
•Annoying
Domain Names
•Simple
IP Addresses
•Easy
Hash Values
•Trivial

Bartle’s Taxonomy of Player Types



Nullcon Goa 2018:- Keynote by Haroon Meer

BRT 5

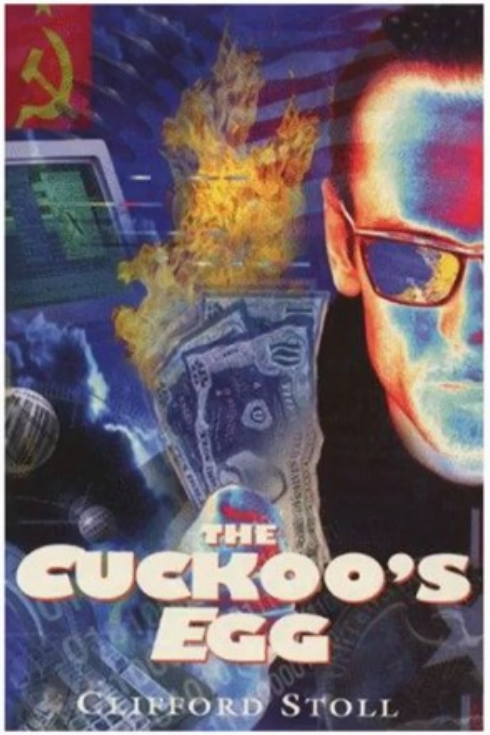
"Turnabout"

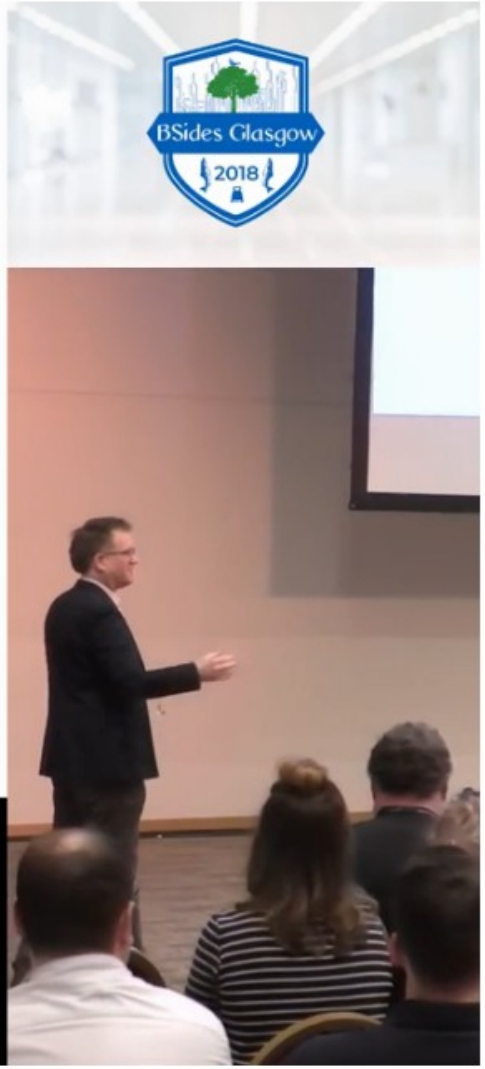
Why should we expect our opponent's decisions to be more rational and coherent than our own?

How quickly we forget how arbitrary, emotional, and unpredictable we ourselves can be.

RECIPROCAL STRATEGIES

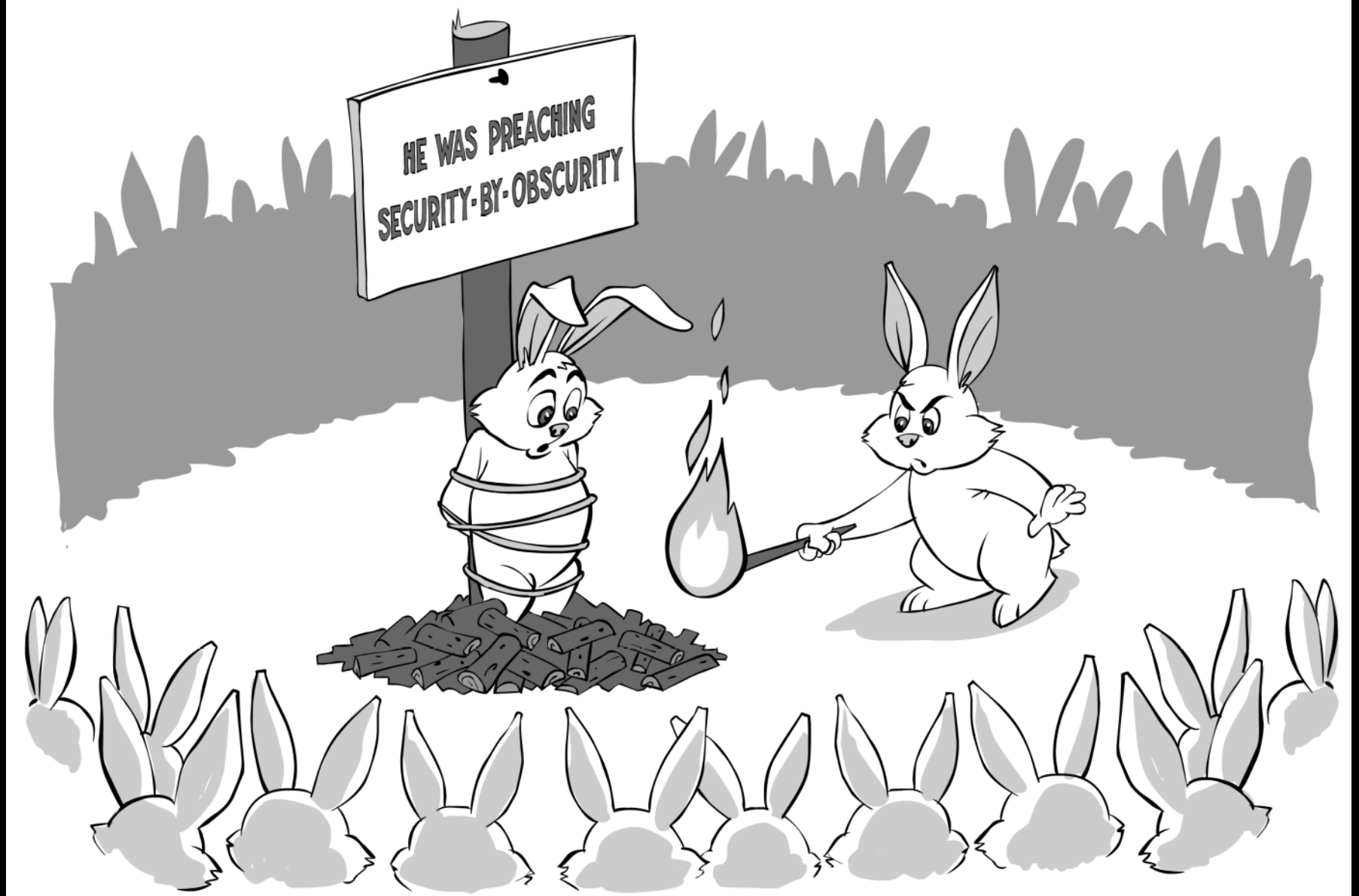
https://www.reciprocalstrategies.com/resources/brt_cards/



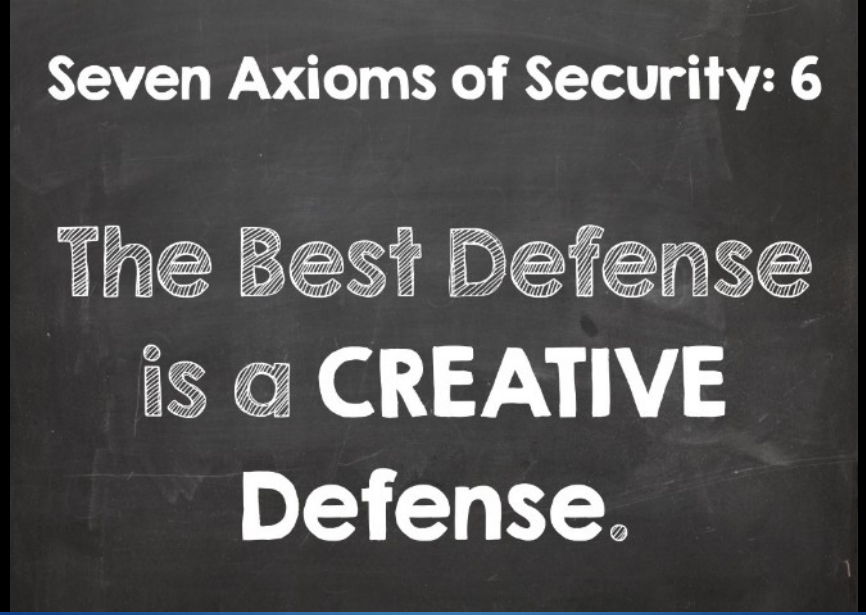


Everyhing You Know Is Wrong - Paul Midian

BSides Glasgow 2018 - Opening Keynote - Everything you know is wrong



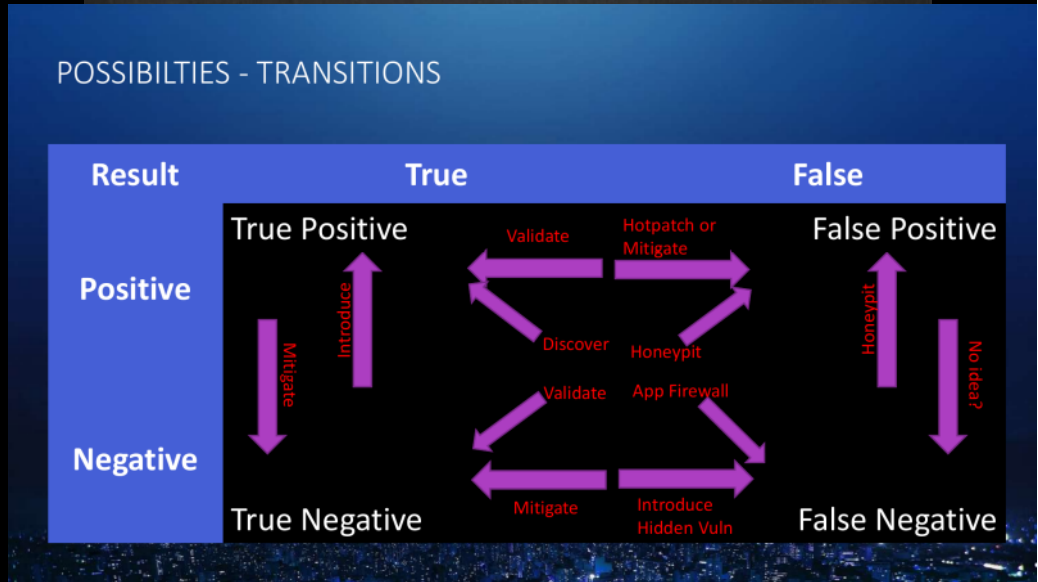
Solving Threat Detection - Alex Davies



Randomly kills instances to test their ability to withstand failure.

It also makes persistence really hard.

70



Defender's Dilemma

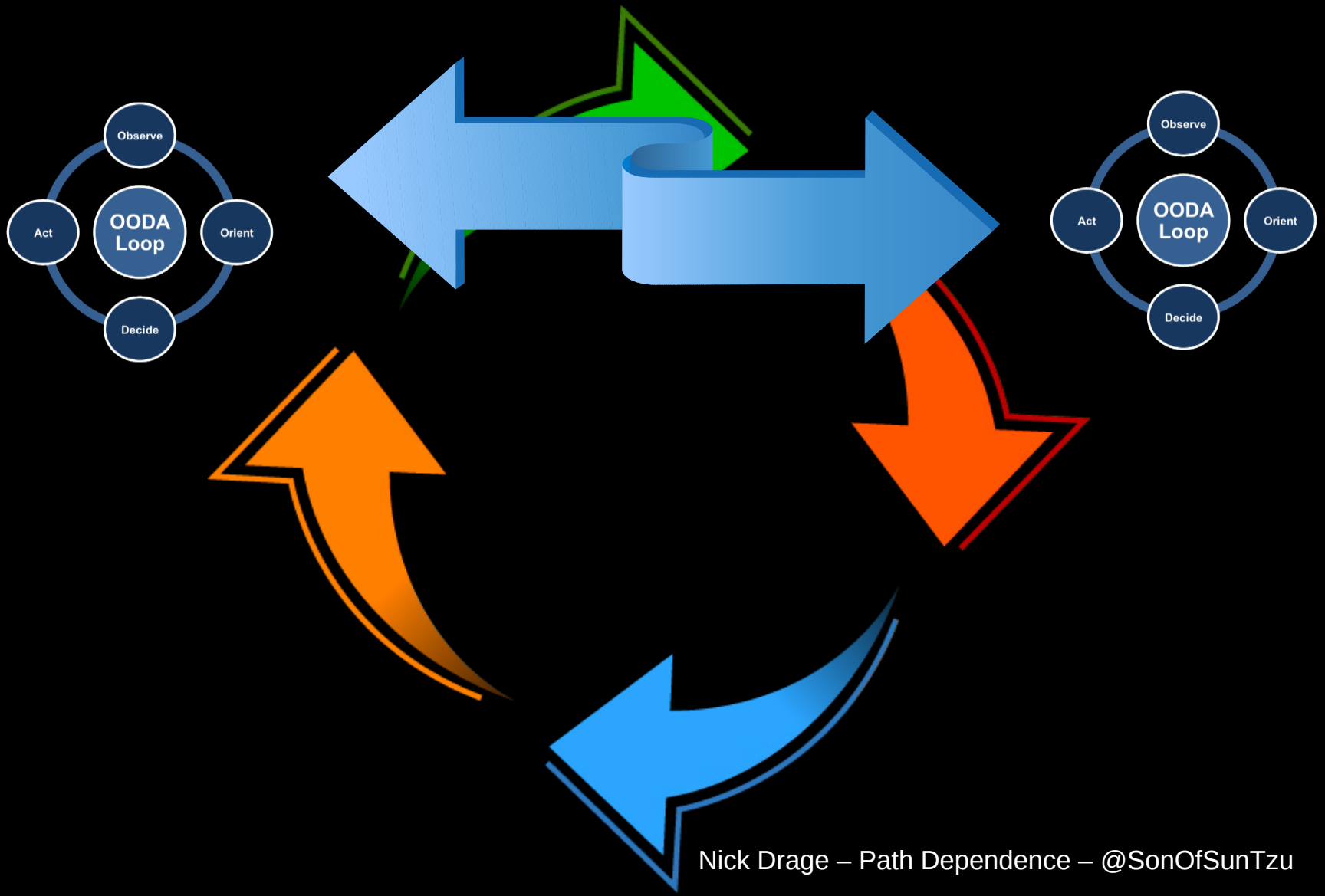
The intruder only needs to exploit one of the victims in order to compromise the enterprise.

Intruder's Dilemma

The defender only needs to detect one of the indicators of the intruder's presence to initiate incident response within the enterprise.

Richard Bejtlich - https://taosecurity.blogspot.de/2009/05/defenders-dilemma-and-intruders-dilemma.html

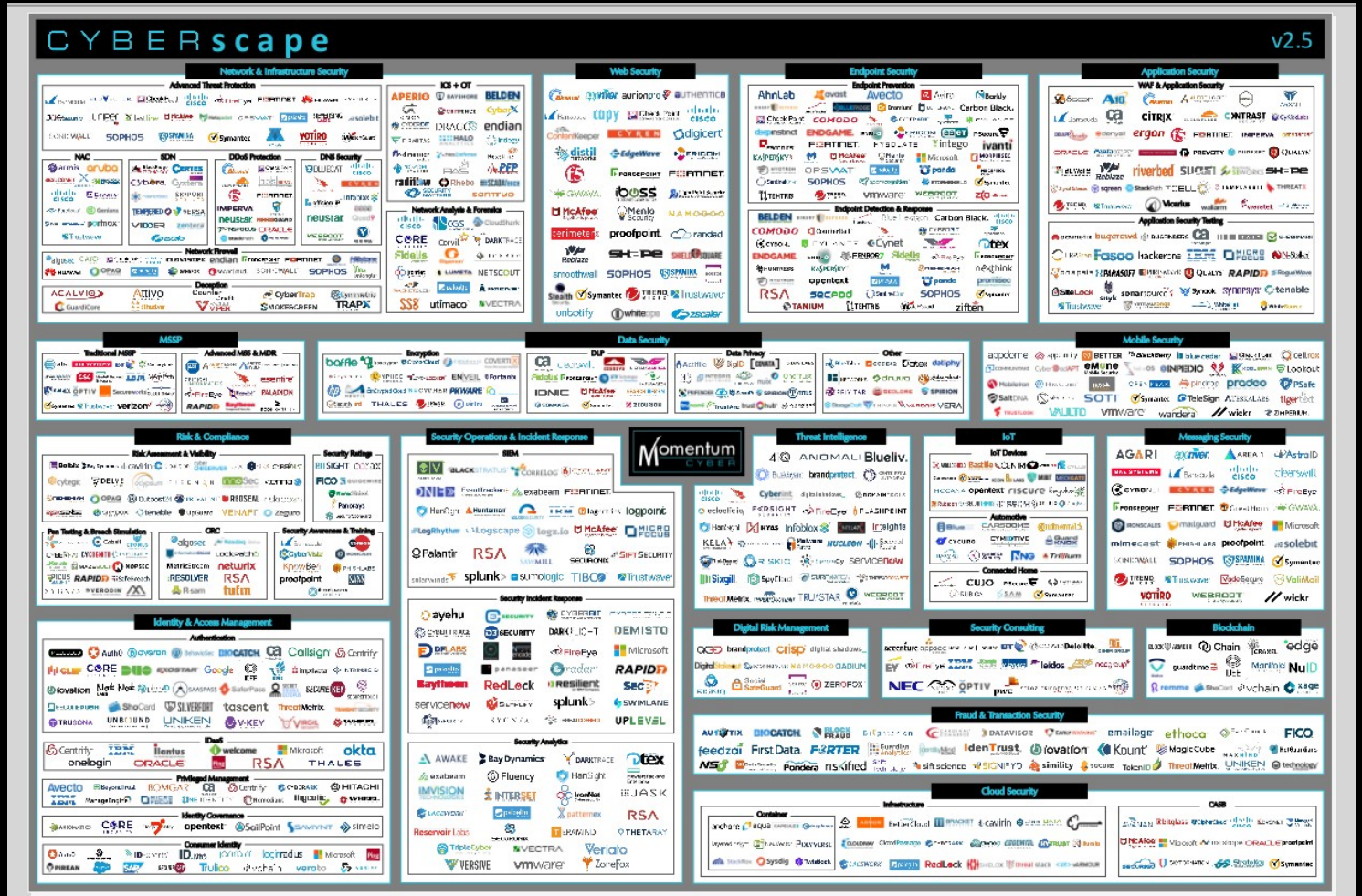
Att&ck™ The Attacker - Christian Kollee


Observe
Act
OODA Loop
Orient
Decide
Observe
Act
OODA Loop
Orient
Decide

Not a blinky box you can buy, install and ignore

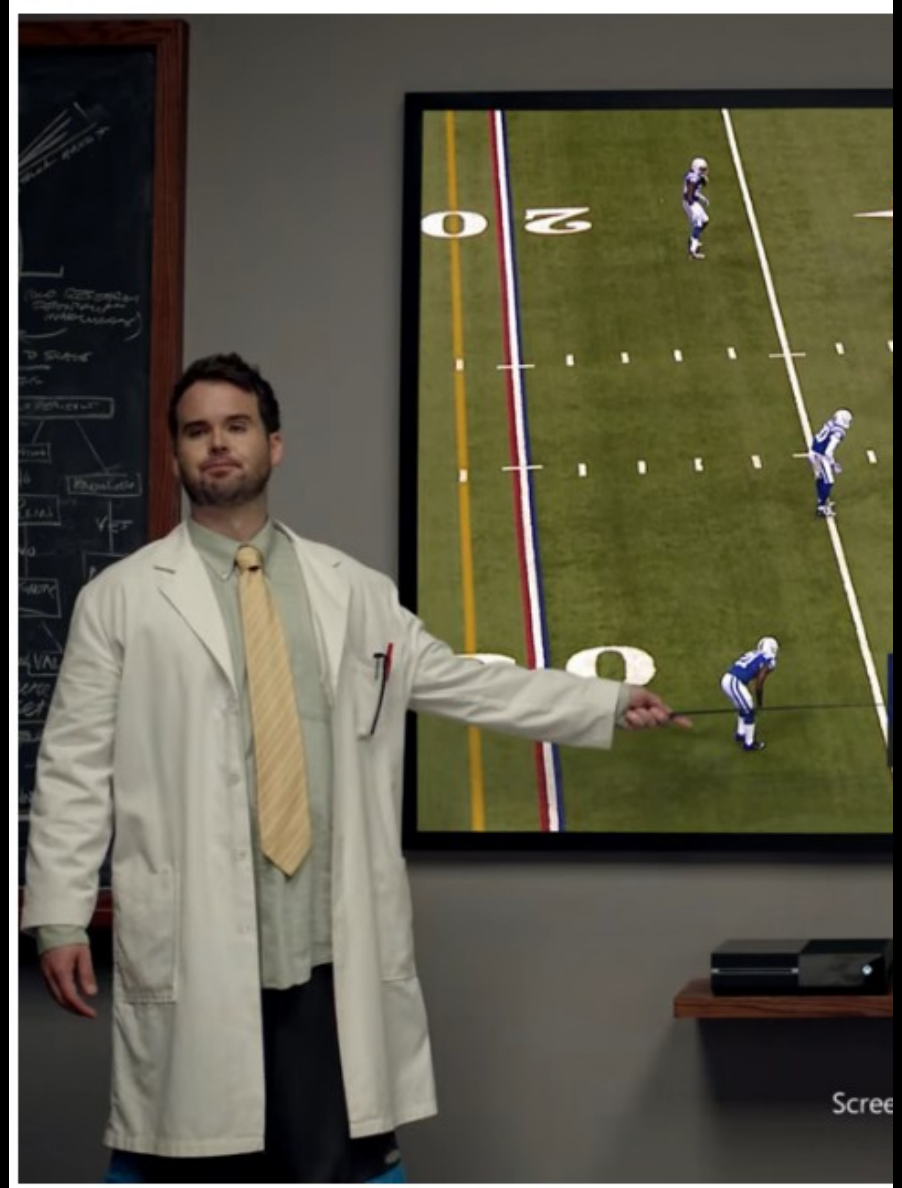
http://www.itpro.co.uk/server/28801/dell-emc-gains-server-market-share-at-hpes-expense

“peak security product”




Sunny Bear - Sun Tzu
@Sunni_Tzu
Follow
Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.
#SunTzu


3RD & 10
NFL.com Fantasy Touchdown
Lazzy Fitzgerald Highlight Available
Press to view
Screens simulated; subject to change.
XBOX



LESSONS

- Use other’s lessons
- Practice Is Everything
- Eliminate the Big Play
- Out Hit Your Opponent

- Or try to Golf our way through American Football...

Nick Drage – Path Dependence – @SonOfSunTzu

Nick Drage - Path Dependence Ltd
nickd@pathdependence.co.uk

blog.sonofsuntzu.org.uk

@SonOfSunTzu