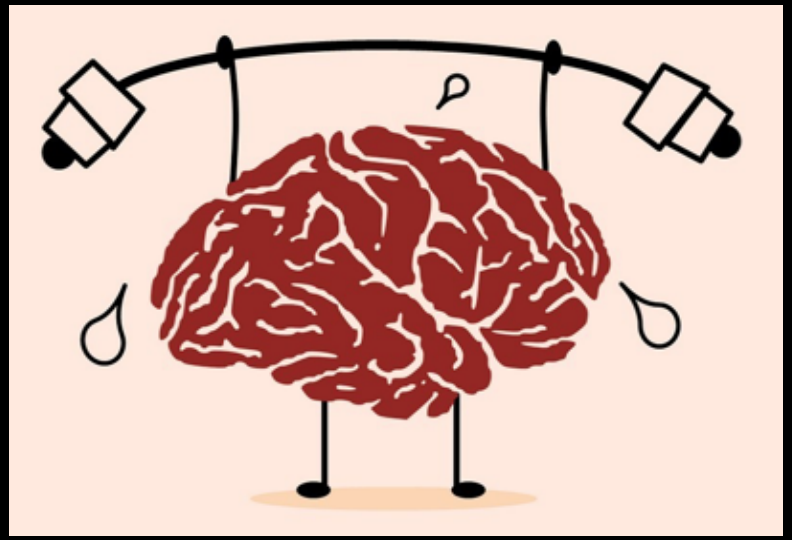
Nick Drage

“Lessons From The Legion”
(The OWASP BeNeLux Remix)

I have a question



You'll Have Questions...

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

The OWASP BeNeLux “Remix” ???

Win the Cyberwar With Zero Trust

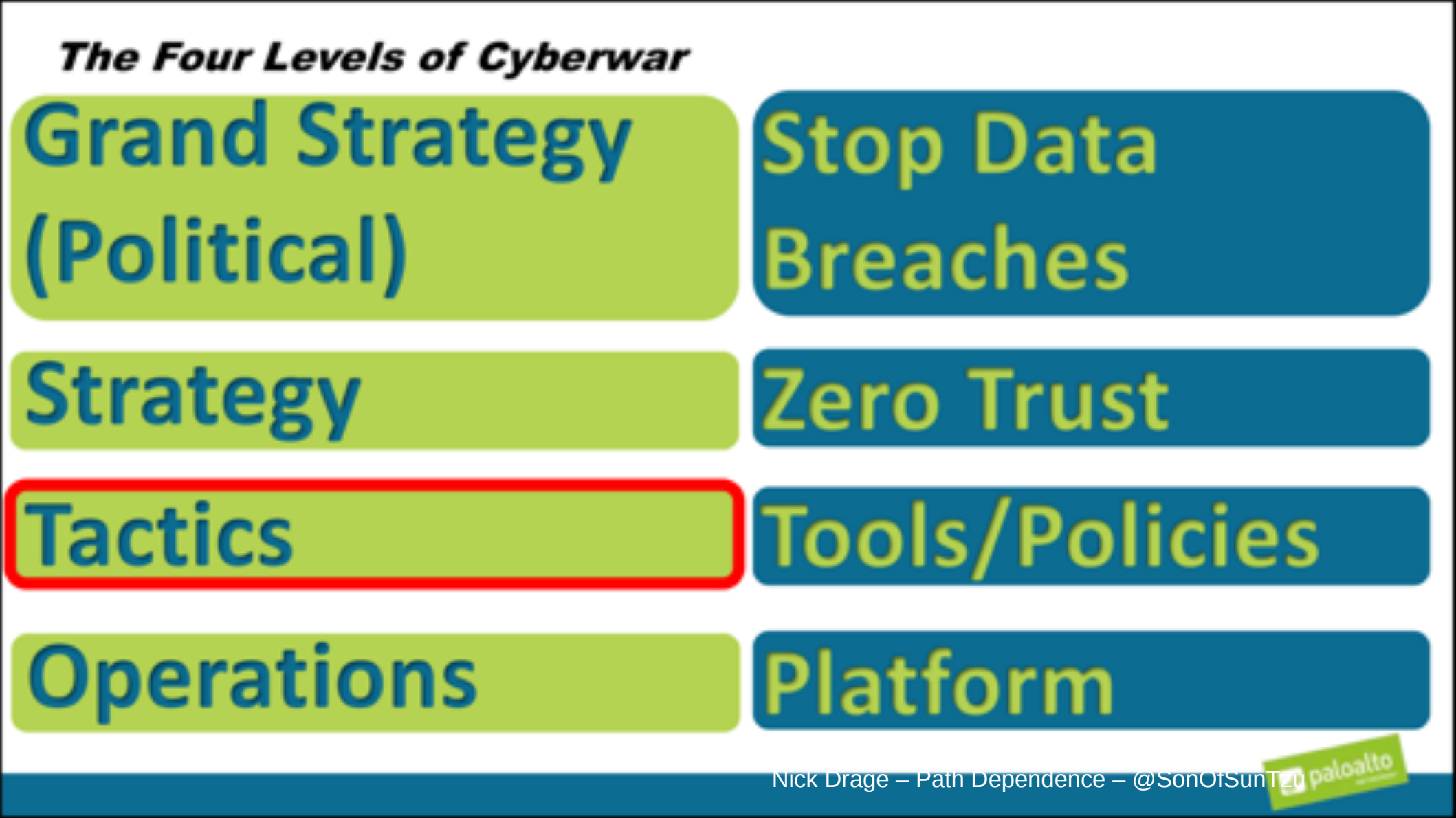
John Kindervag

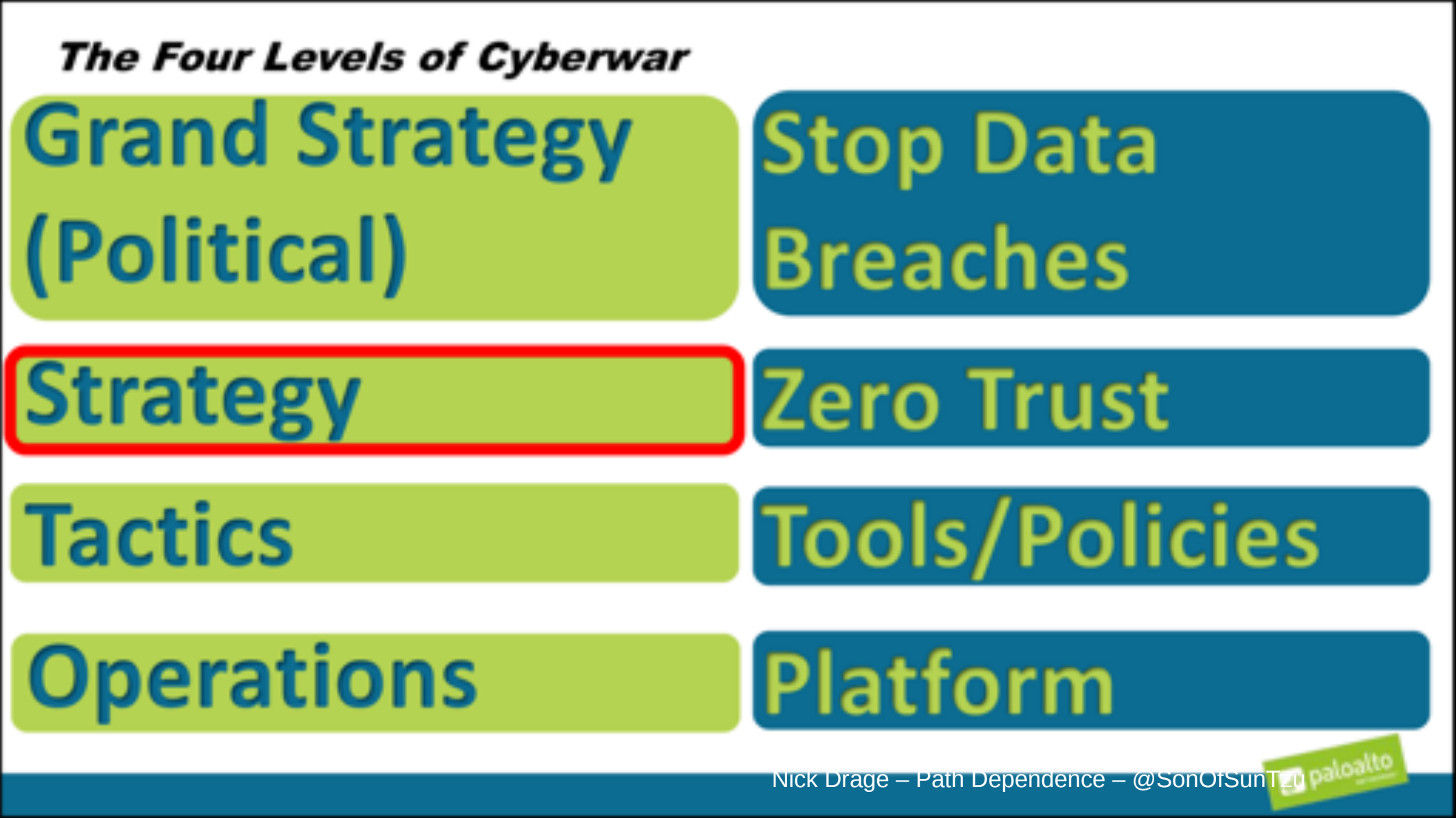
Field CTO

Nick Drage – Path Dependence – @SonOfSunTzu

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

Tactics

- System Administrators
- Developers
- Security Operations

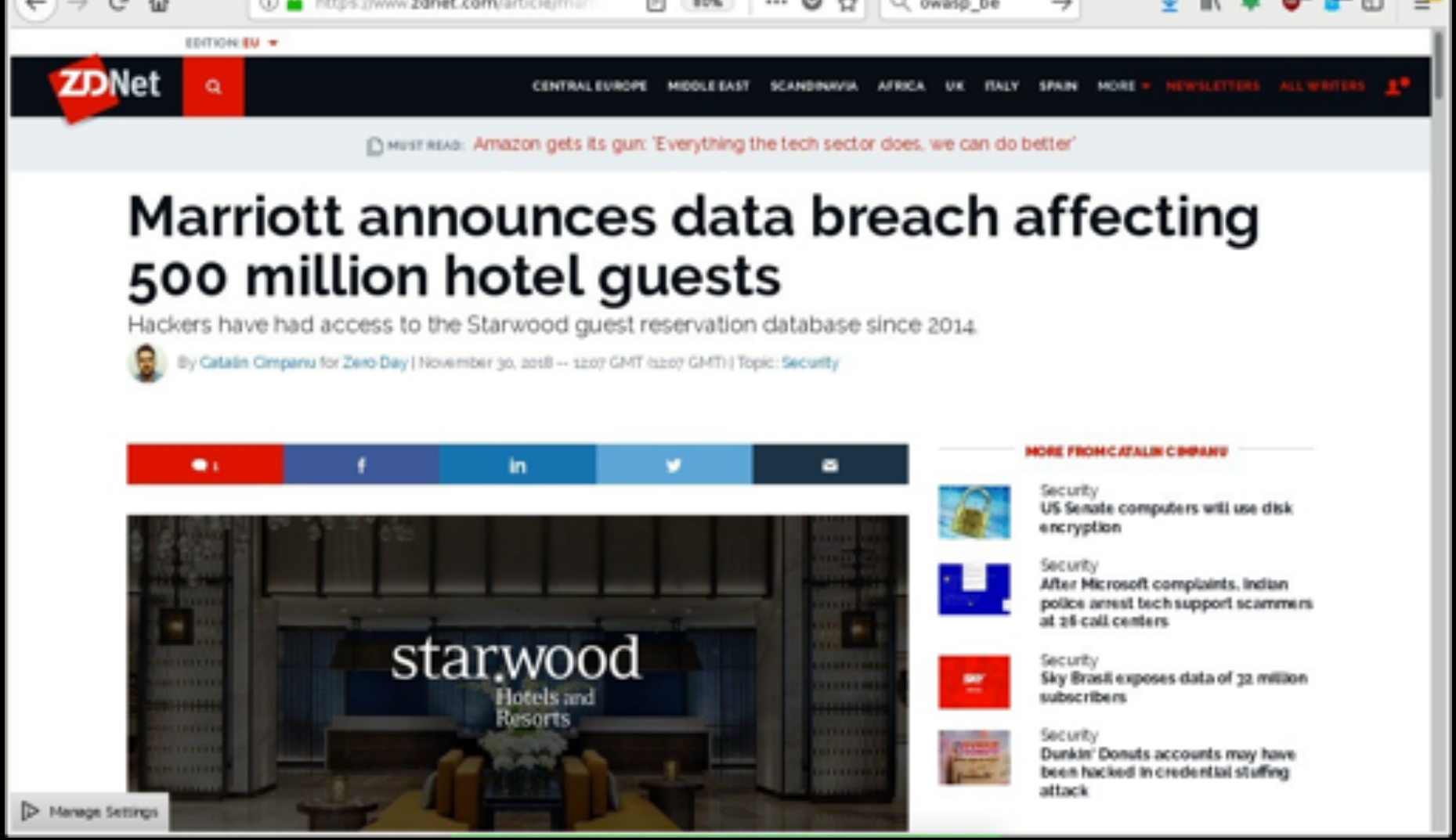
How do we learn and train

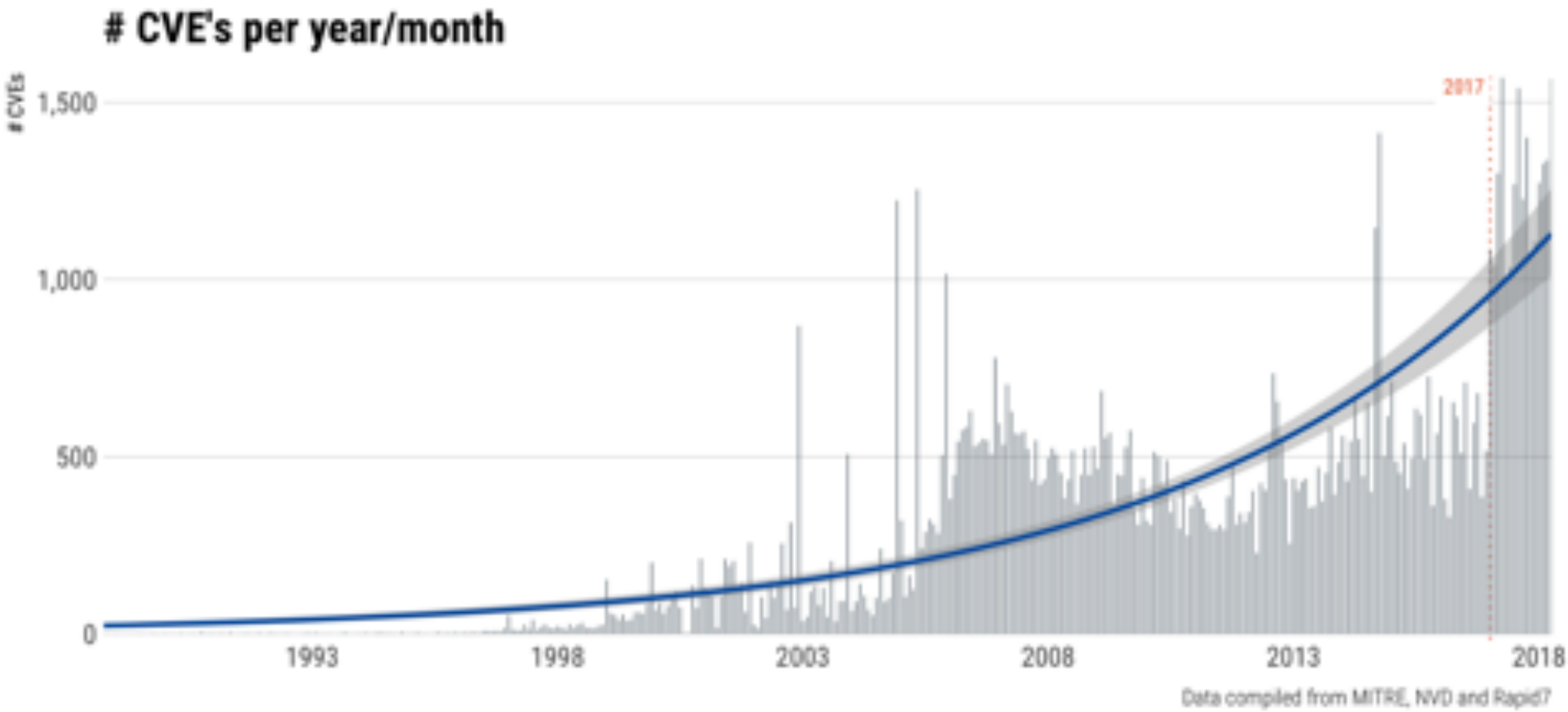
Nick Drage – Path Dependence – @SonOfSunTzu

Matt Wiebe - a lonely robot - https://www.flickr.com/photos/mattwieve/29221303838 CC2.0

BreachLevelIndex.com

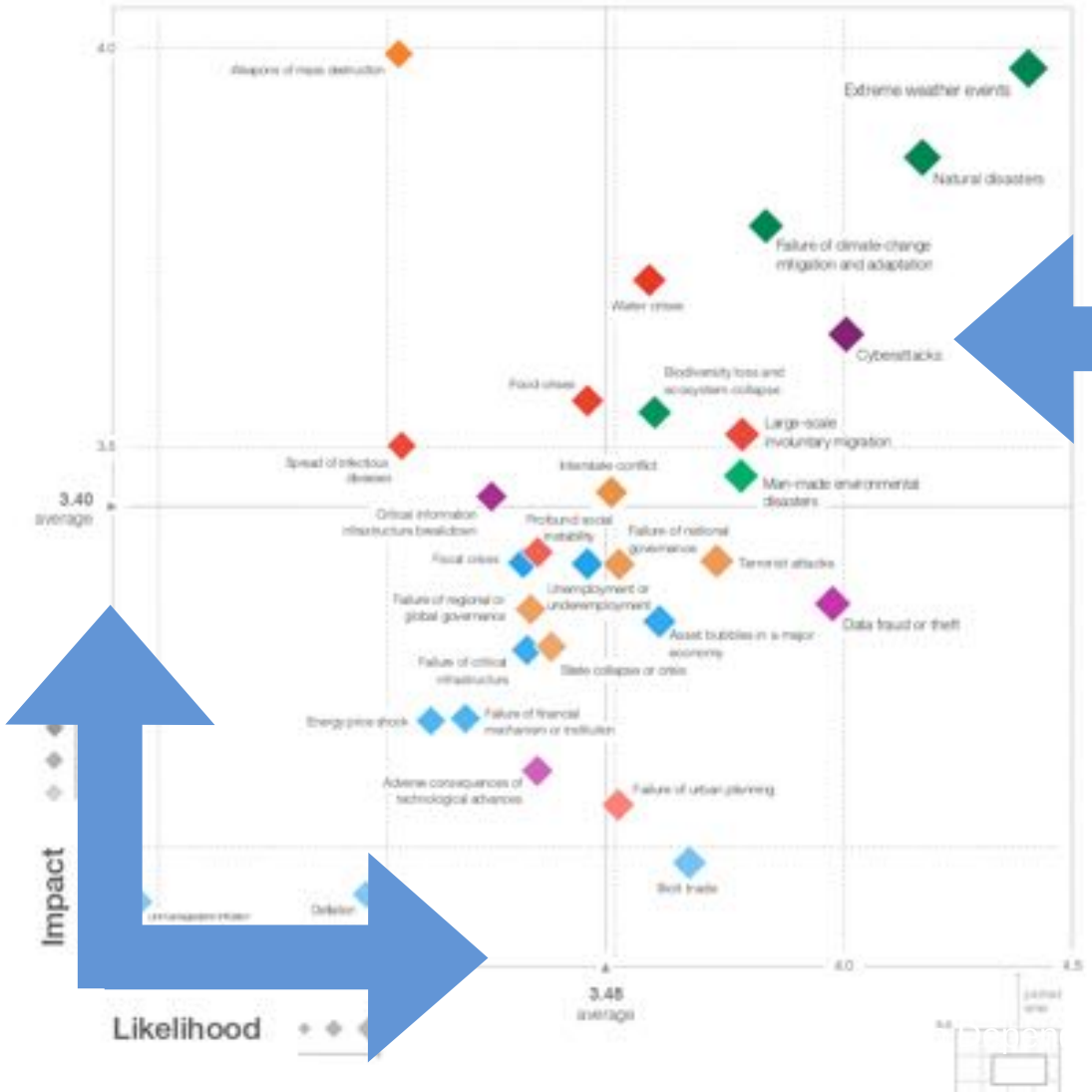
BreachLevelIndex.com


EDITION: EU
ZDNet
CENTRAL EUROPE
MIDDLE EAST
SCANDINAVIA
AFRICA
UK
ITALY
SPAIN
MORE
NEWSLETTERS
ALL WRITERS
MUST READ: Amazon gets its gun: 'Everything the tech sector does, we can do better'
Marriott announces data breach affecting 500 million hotel guests
Hackers have had access to the Starwood guest reservation database since 2014
By Catalin Cimpanu for Zero Day | November 30, 2018 -- 12:07 GMT (12:07 GMT) | Topic: Security
starwood
Hotels and Resorts
MORE FROM CATALIN CIMPANU
Security
US Senate computers will use disk encryption
Security
After Microsoft complaints, Indian police arrest tech support scammers at 28 call centers
Security
Sky Brasil exposes data of 32 million subscribers
Security
Dunkin' Donuts accounts may have been hacked in credential stuffing attack
Manage Settings


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

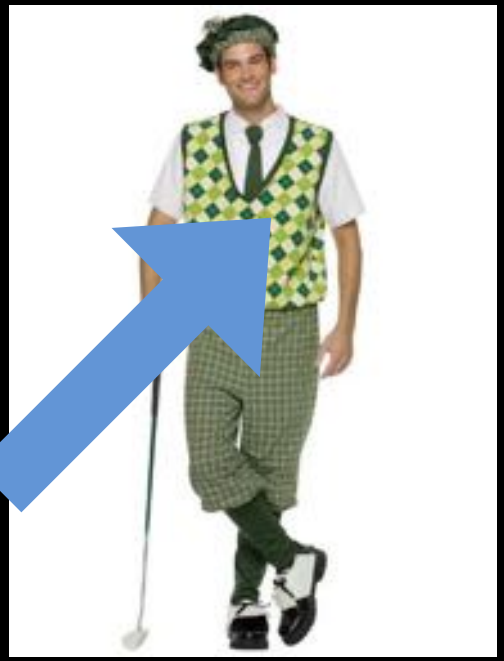
Figure I: The Global Risks Landscape 2018



What’s wrong

- Nothing wrong with golf
- … or training for golf
- … if you’re going to play golf.

Image: Costume SuperCentre

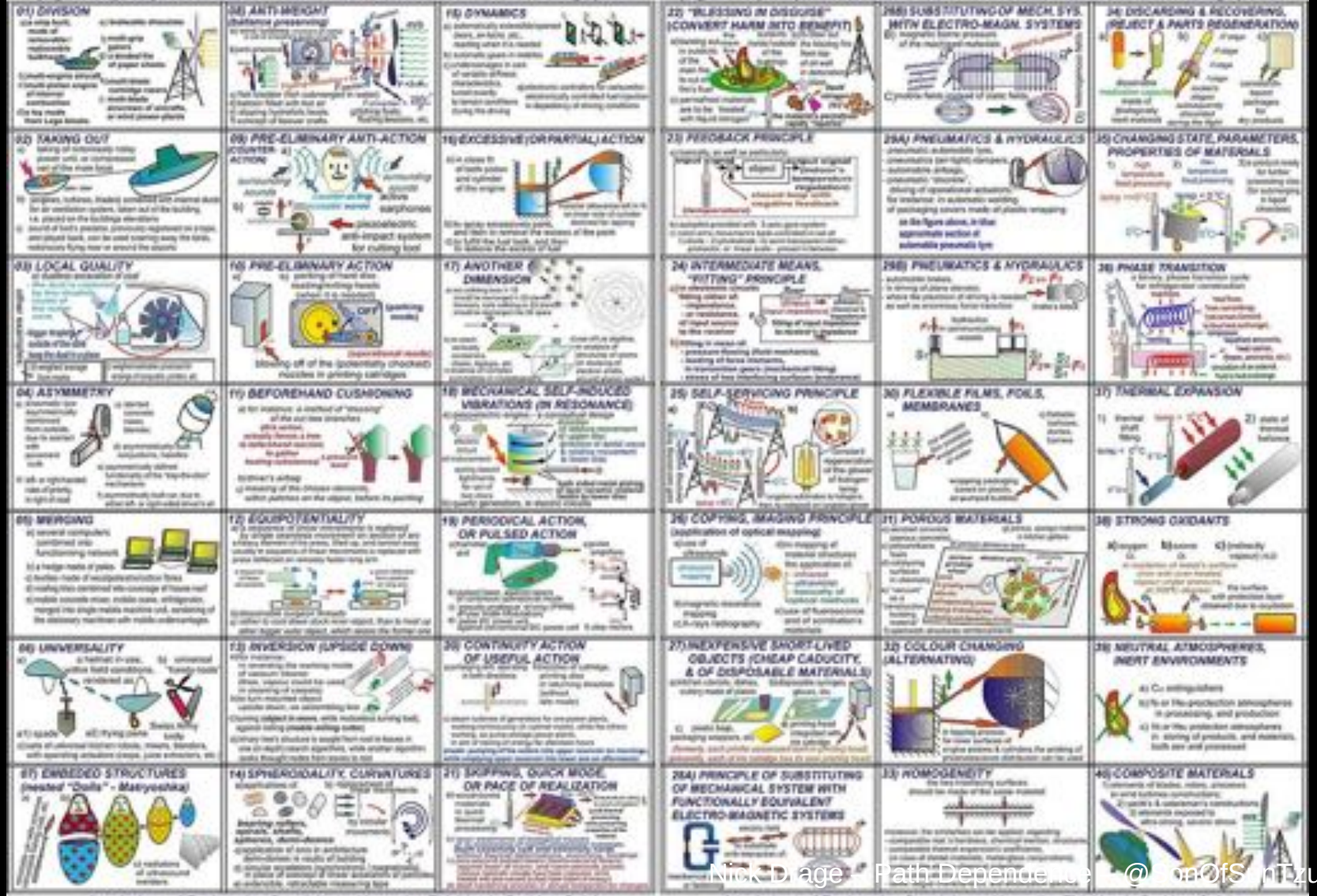


Nick Drage – Path Dependence – @SonOfSunTzu

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

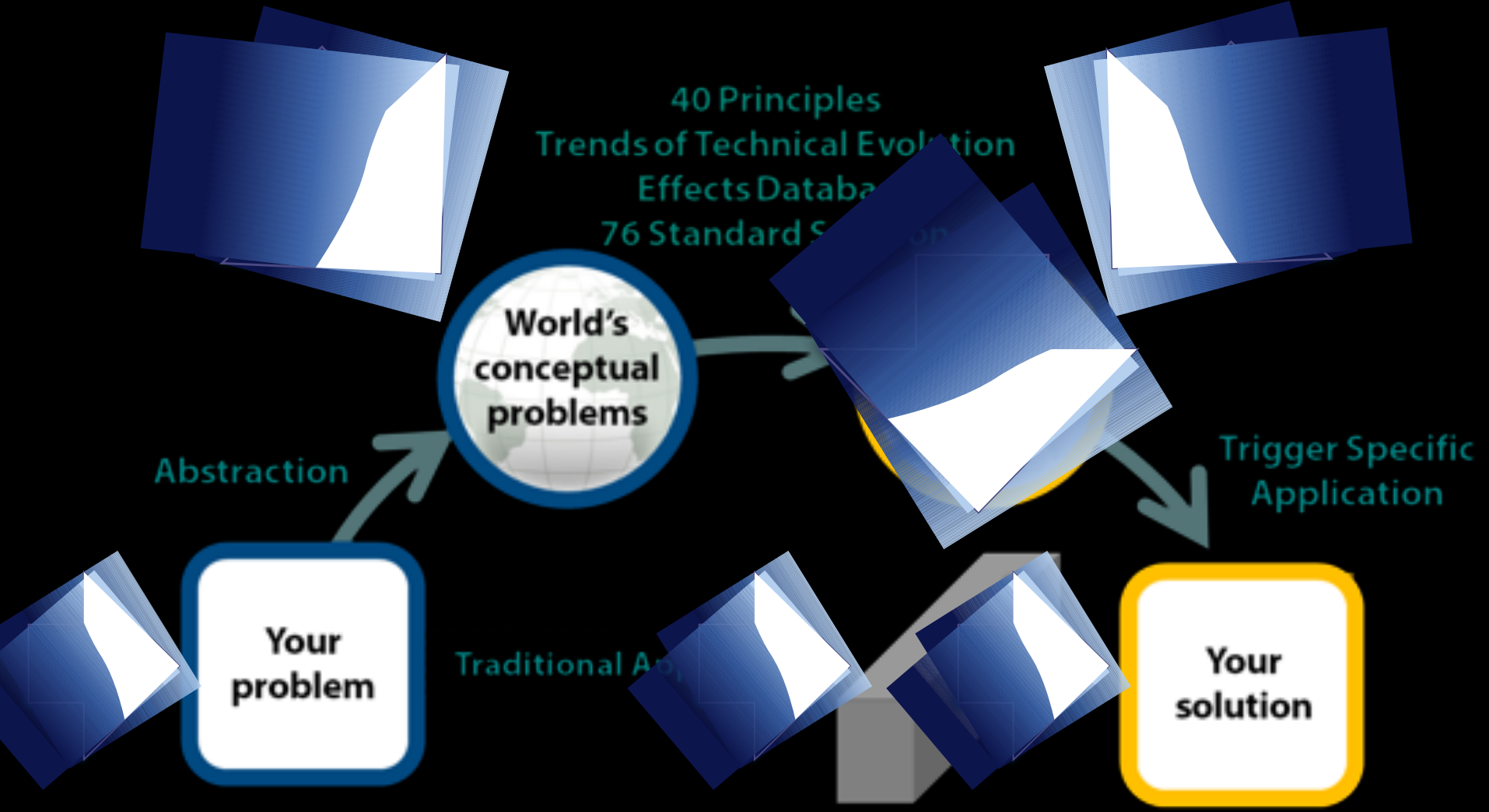
TRIZ

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



page B - 40 principles of invention in TRIZ method, sketches rendered into vector graphics

A technique of Engineering Creativity and Inventive Thinking in Problem Solving

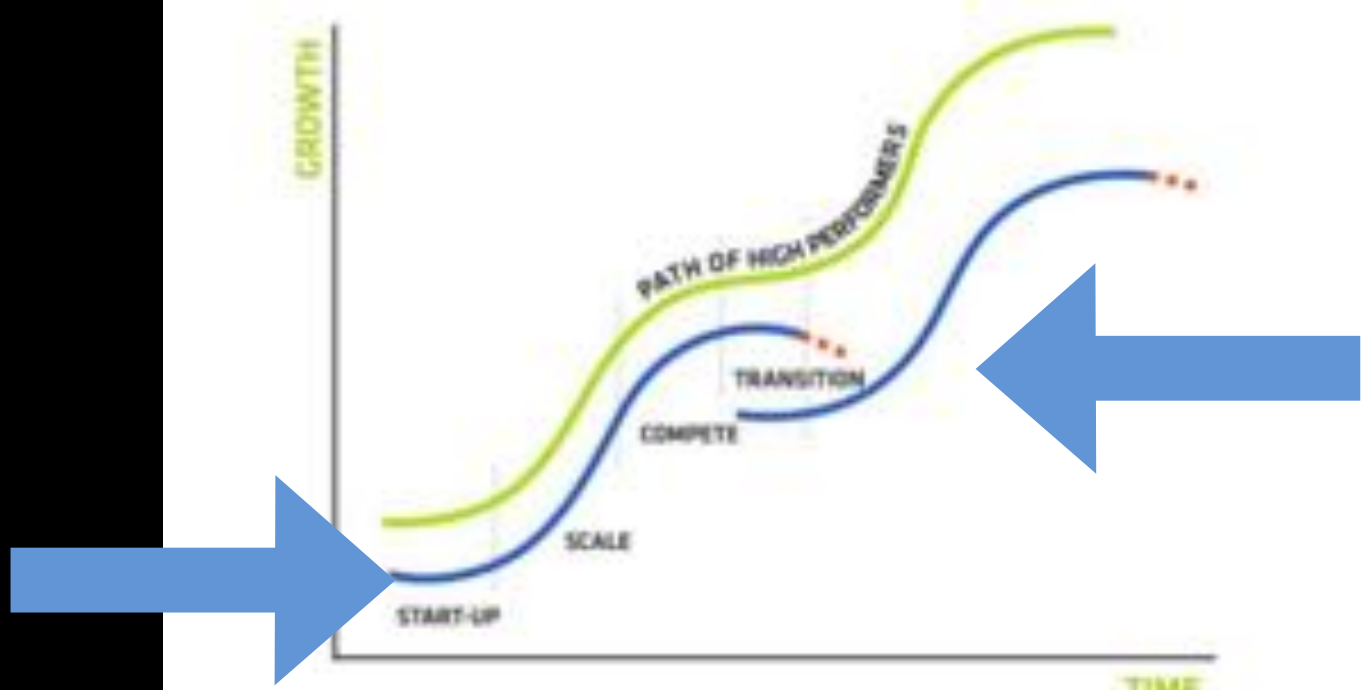


Darrell Mann:
“… more extreme versions of your problem ...”

Image: Murali Loganathan

Strategic Inflection Point

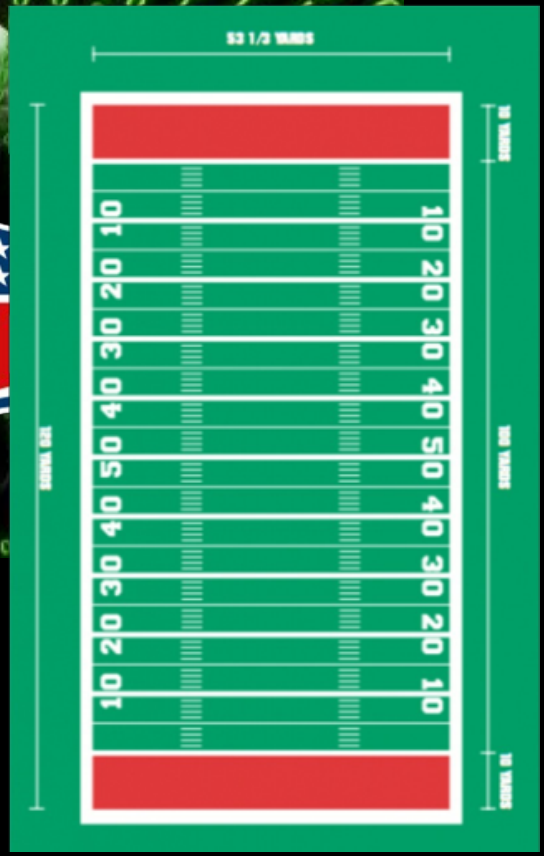
Double S-Curve Needs!



So ...

Nick Drage – Path Dependence – @SonOfSunTzu

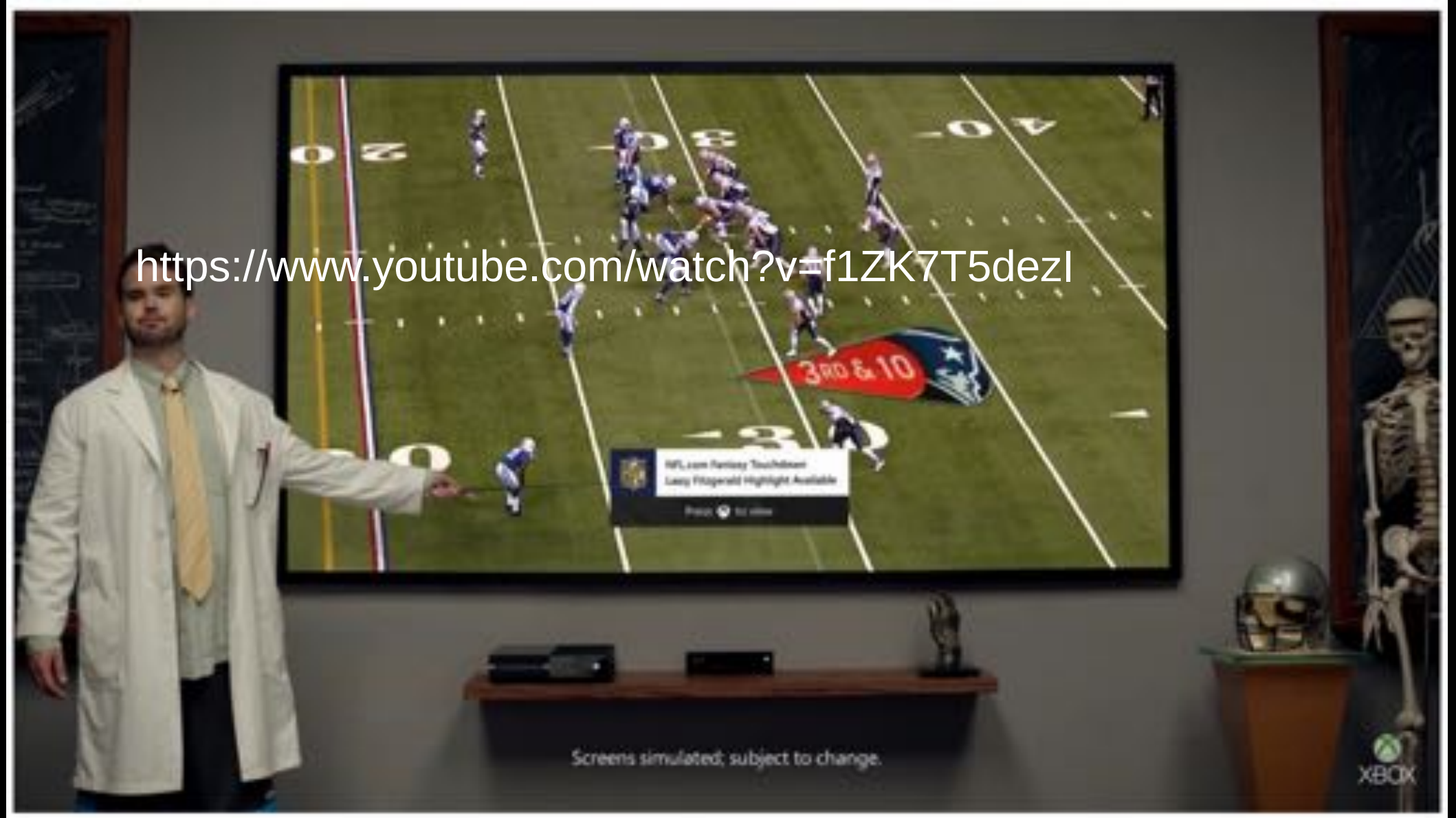
- Utterly incomprehensible from outside
- Complex
- Team games
- Highly specialised
  - By situation
  - Attack or Defend
- Offensive or defensive playbooks
- Fight over territory



https://media.defense.gov/

“Rice said she was attracted to two fundamental similarities between football and warfare: the use of strategy and the goal of taking territory.” - NY Times

Nick Drage – Path Dependence – @SonOfSunTzu


https://www.youtube.com/watch?v=f1ZK7T5dezI
3RD & 10
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

Nick Drage – Path Dependence – @SonOfSunTzu

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

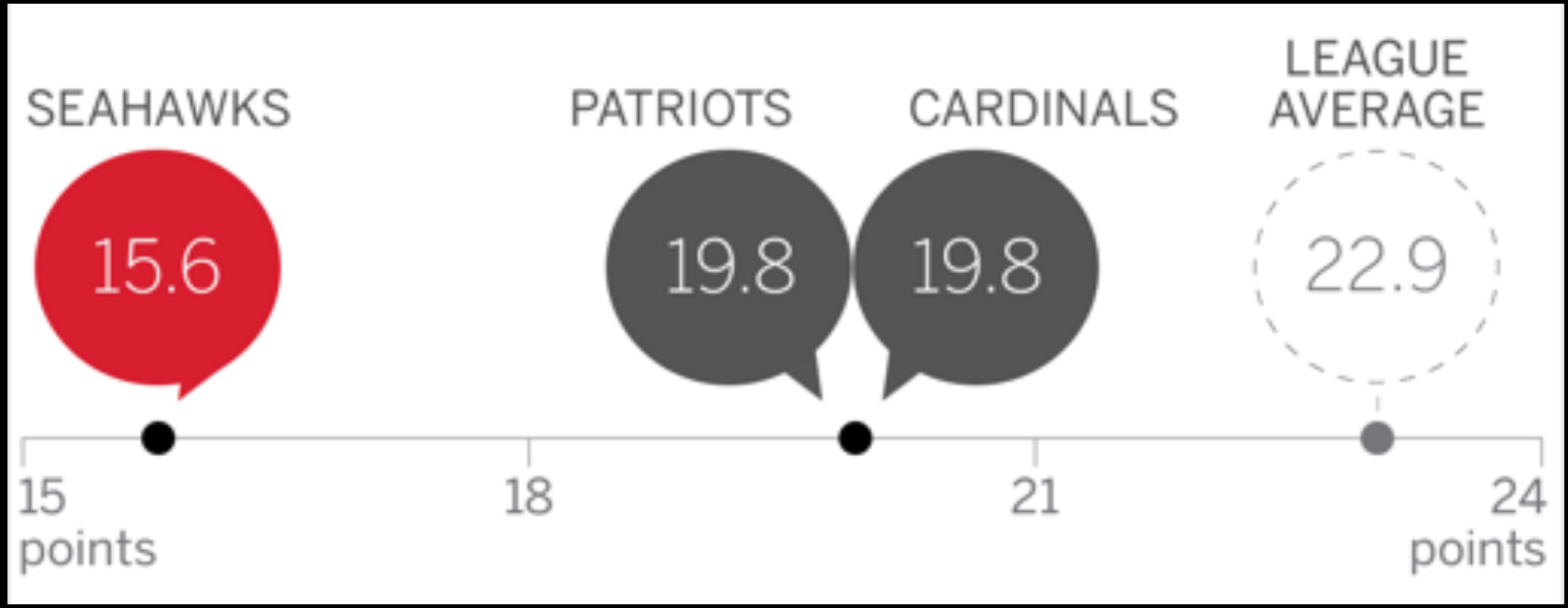


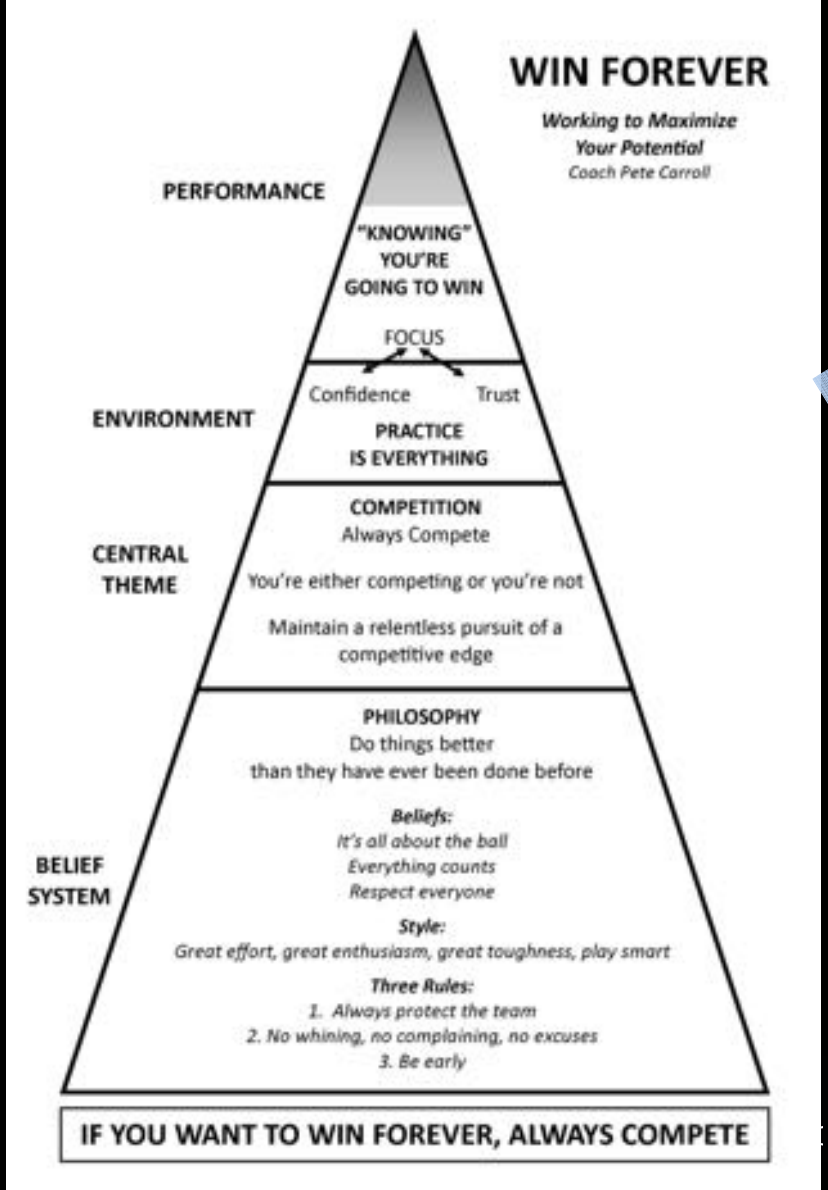
Image: ESPN

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 – “Shift Left” Your Conflict

PRACTICE IS EVERYTHING




SUPER BOWL XLVIII CHAMPIONS
SUPER BOWL XLVIII
SUPER BOWL XLVIII
Nick Drage – Path Dependence – @SonOfSunTzu

Offense			3rd String
QB			Terrelle Pryor
HB			
HB2			
	Coleman	Ware	Kiero Small
	Miller	Anthony McCoy	
WR		Paul	Bryan Waters
WR2			Ricardo Lockette
SWR			
LT			
LG			
C			Greg Van Roten
RG			
RT	Michael	Britt	

Defense	Start	ng	3rd String
DLE			Benson Mayowa
DLT			Jordan Hill/D'Anthony Smith
DRT			Jimmy Staten
DRE			O'Brien Schofield
SLB			
MLB		Heath	
WLB		Michael	Kevin Pierre-Louis
LCB	Sherman	Tharold Simo	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

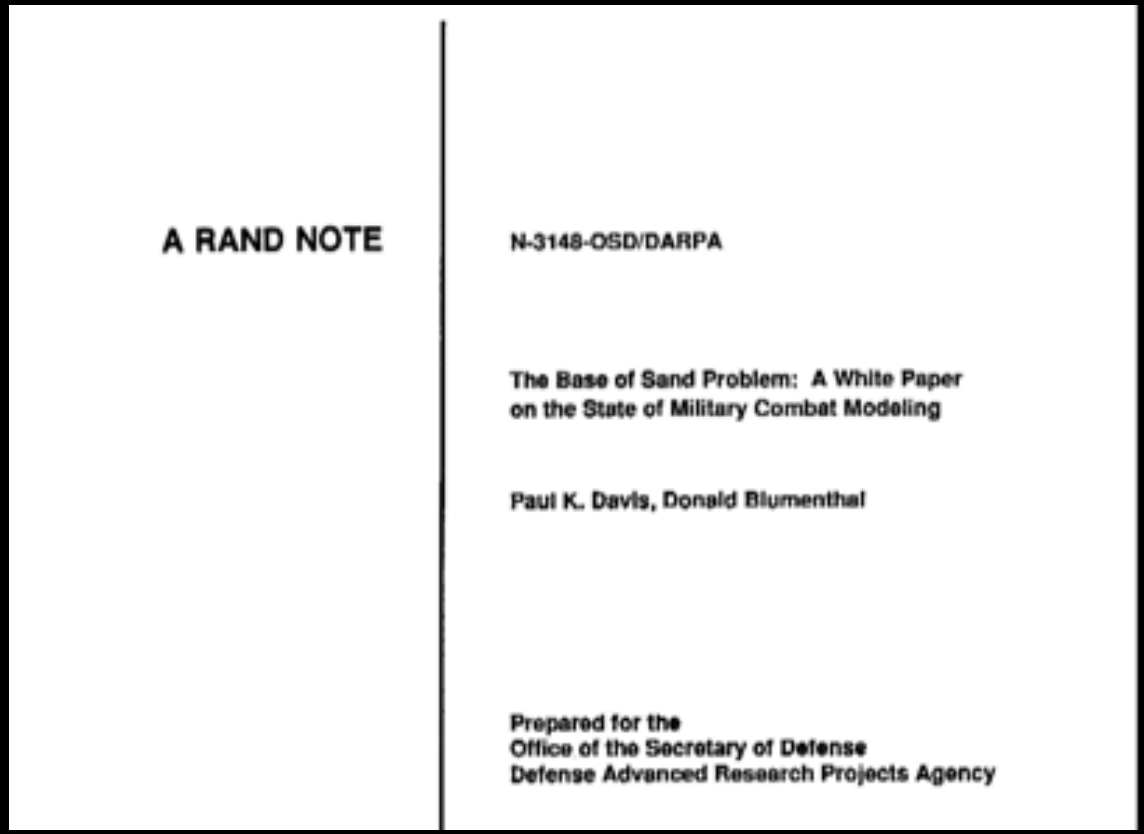
Trap #10: Threat Modeling at the Wrong Time


OWASP
Zed Attack Proxy

Image: @rubentroncon

Image: @OWASP_BE

The Base of Sand Problem



A RAND NOTE

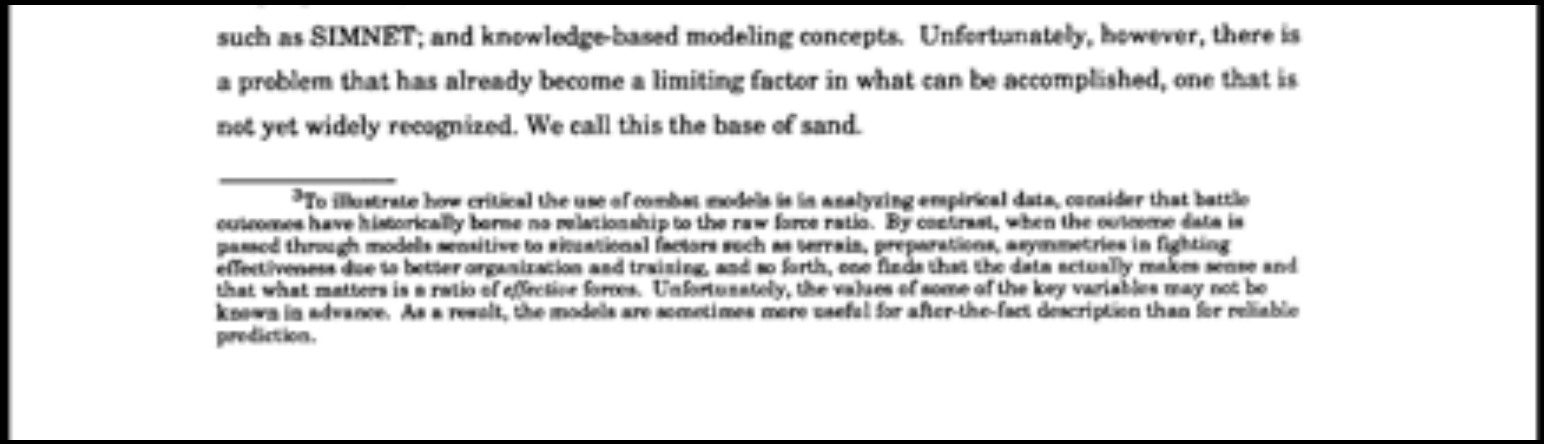
N-3148-OSD/DARPA

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)

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

Jeremiah Grossman

CEO of Bit Discovery, Professional Hacker, Black Belt in Brazilian Jiu-Jitsu, Off-Road Race Car Driver, Founder of WhiteHat Security, and Maui resident.

MONDAY, MAY 07, 2018

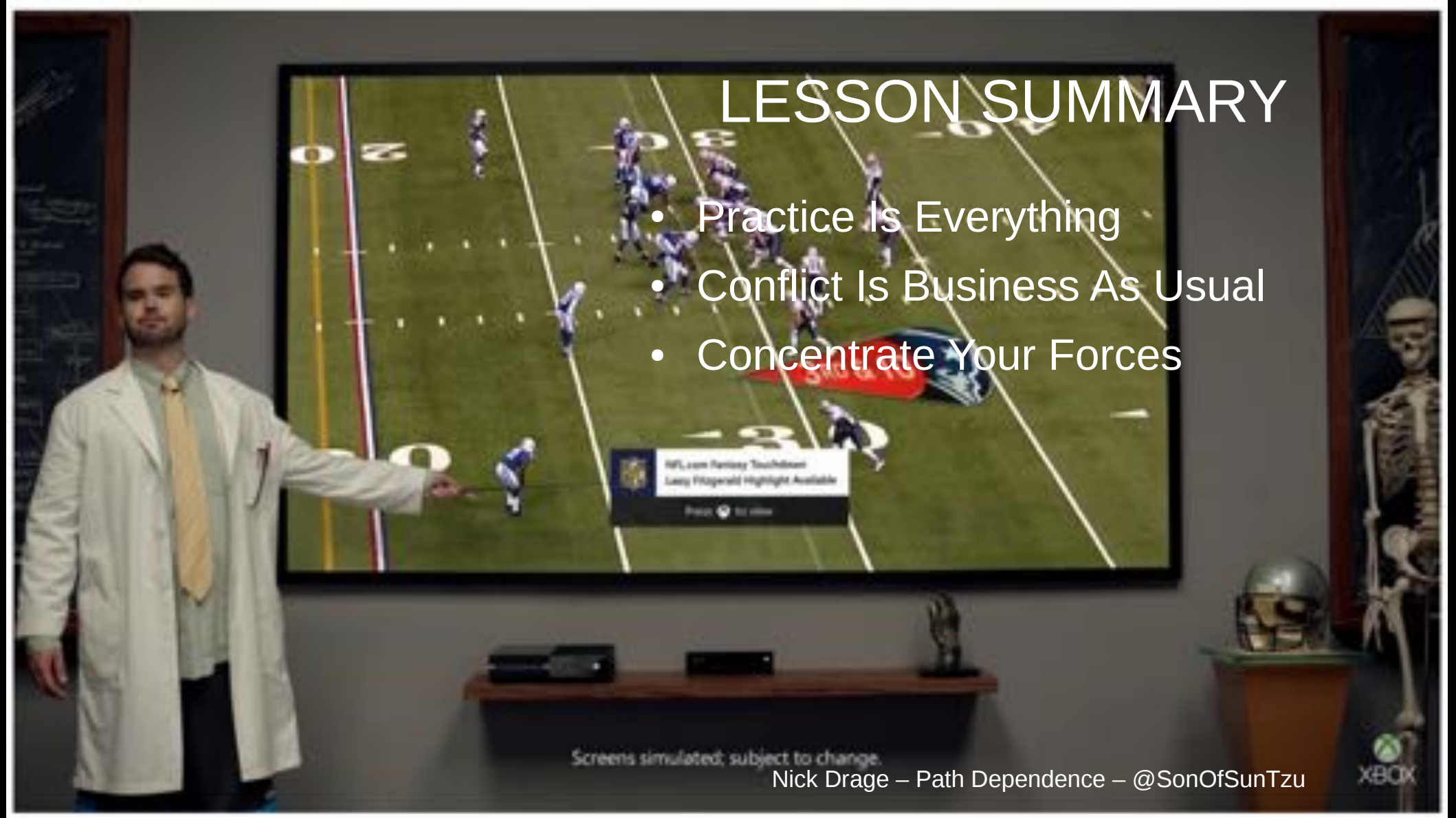
All these vulnerabilities, rarely matter.

There is a serious misalignment of interests between Application Security vulnerability assessment vendors and their customers. Vendors are incentivized to report everything they possible can, even issues that rarely matter. On the other hand, customers just want the vulnerability reports that are likely to get them hacked. Every finding beyond that is a waste of time, money, and energy, which is precisely what's happening every day. Let's begin exploring this with some context:

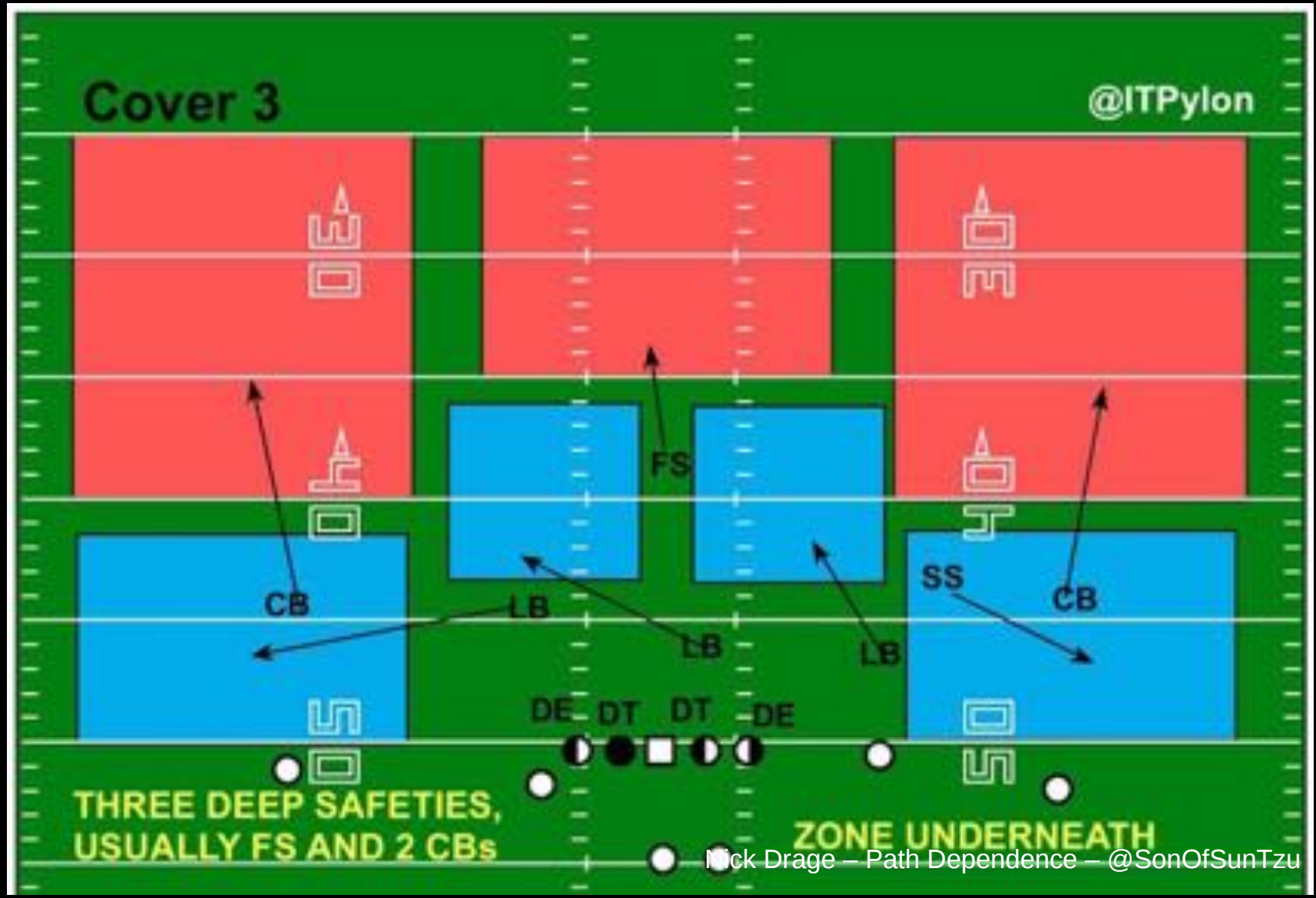
ABOUT ME

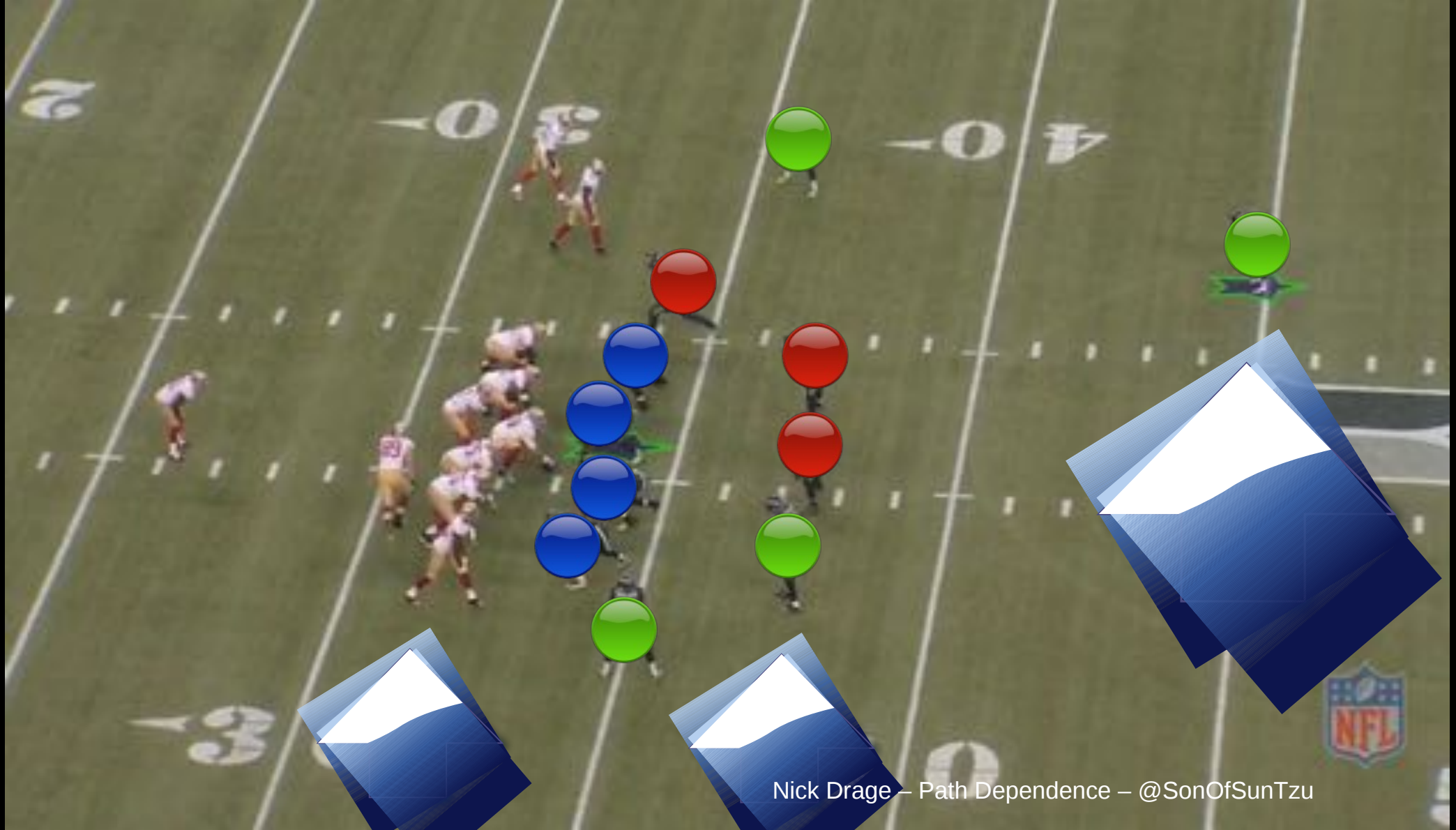
Jeremiah Grossman

Jeremiah Grossman's career spans nearly 20 years and has lived a literal lifetime in computer security to become one of the industry's biggest

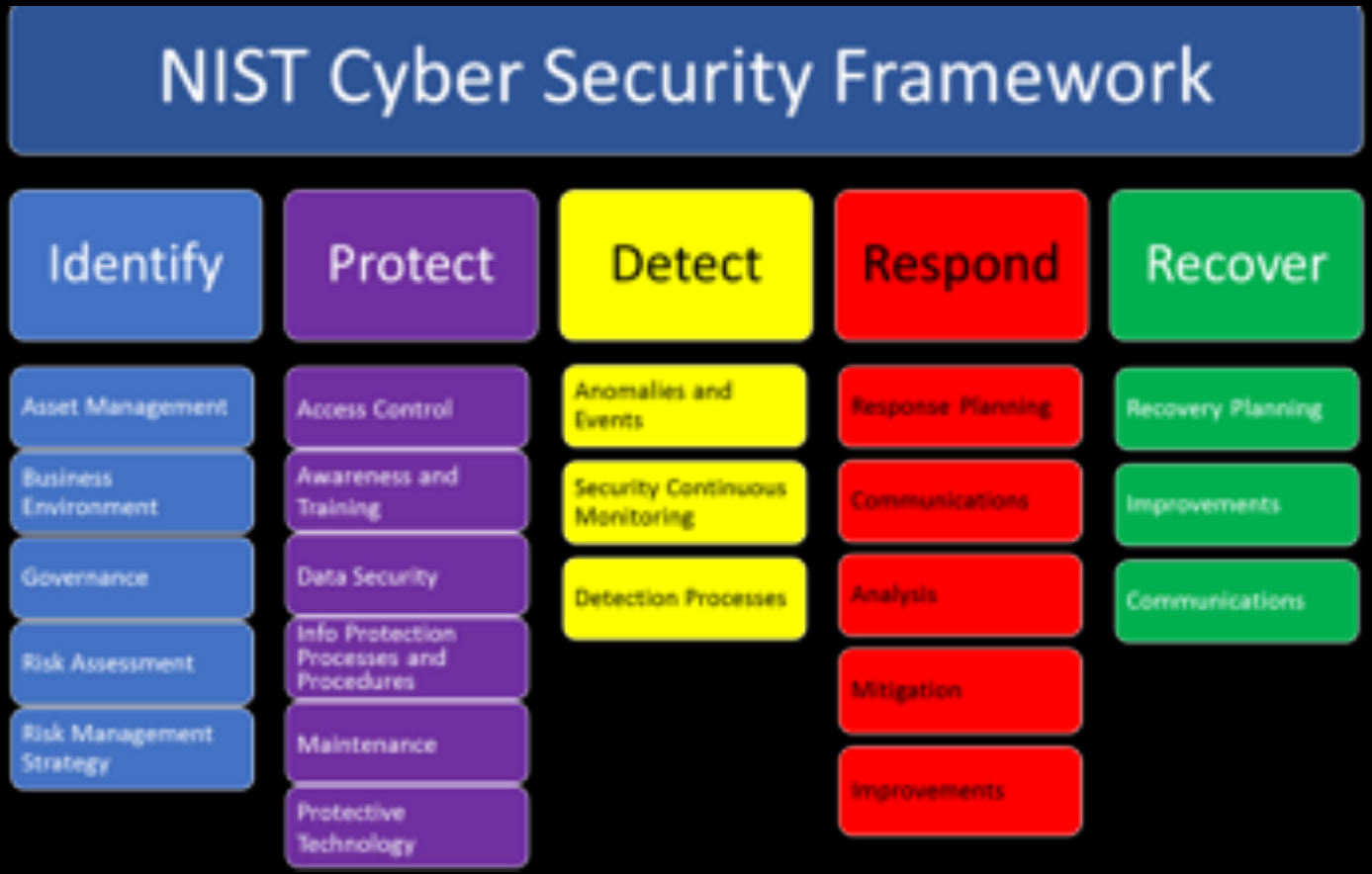

LESSON SUMMARY
• Practice Is Everything
• Conflict Is Business As Usual
• Concentrate Your Forces
Screens simulated; subject to change.
XBOX

LESSON – Eliminate The Big Play


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


Nick Drage – Path Dependence – @SonOfSunTzu

NIST – five core functions



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

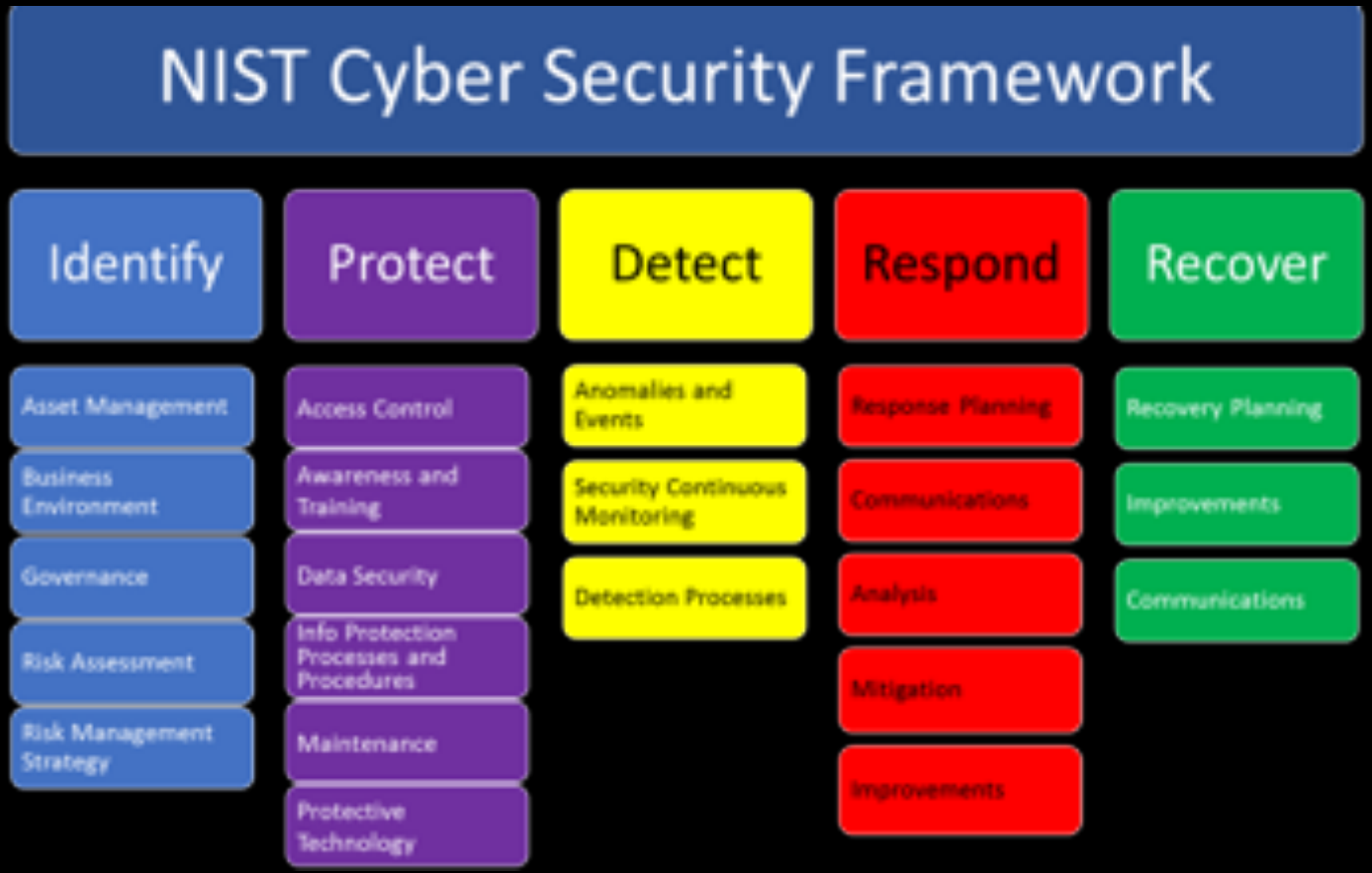
NIST – five core functions

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

NIST – five core functions

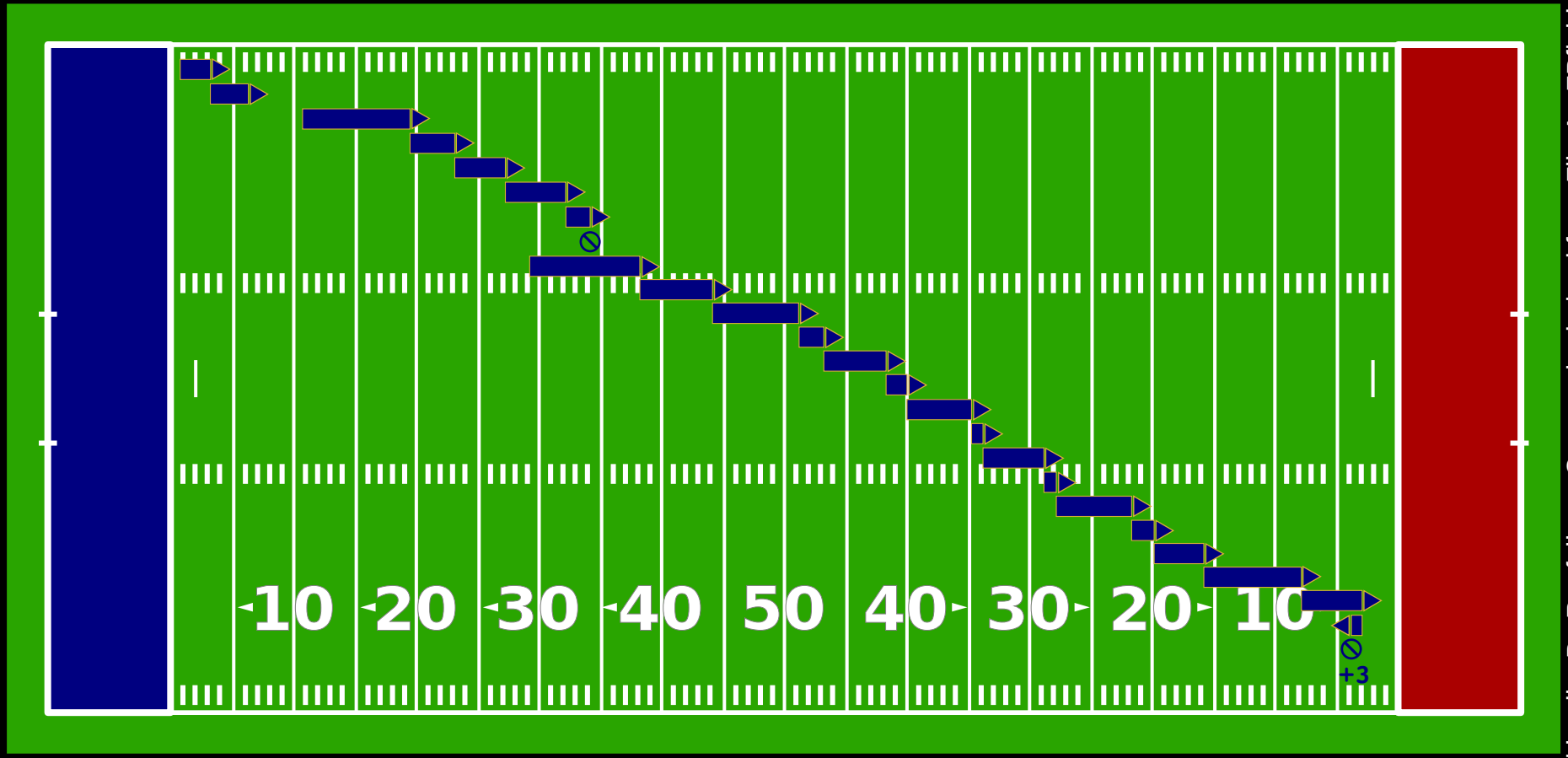
https://medium.com/@TechTieu/cyber-security-framework-66aa07c1b7a5

NIST – five core functions



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

Drive chart



Nick Drage – Path Dependence – @SonOfSunTzu

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

How breaches work (perception vs reality)

Getting hacked (common perception)

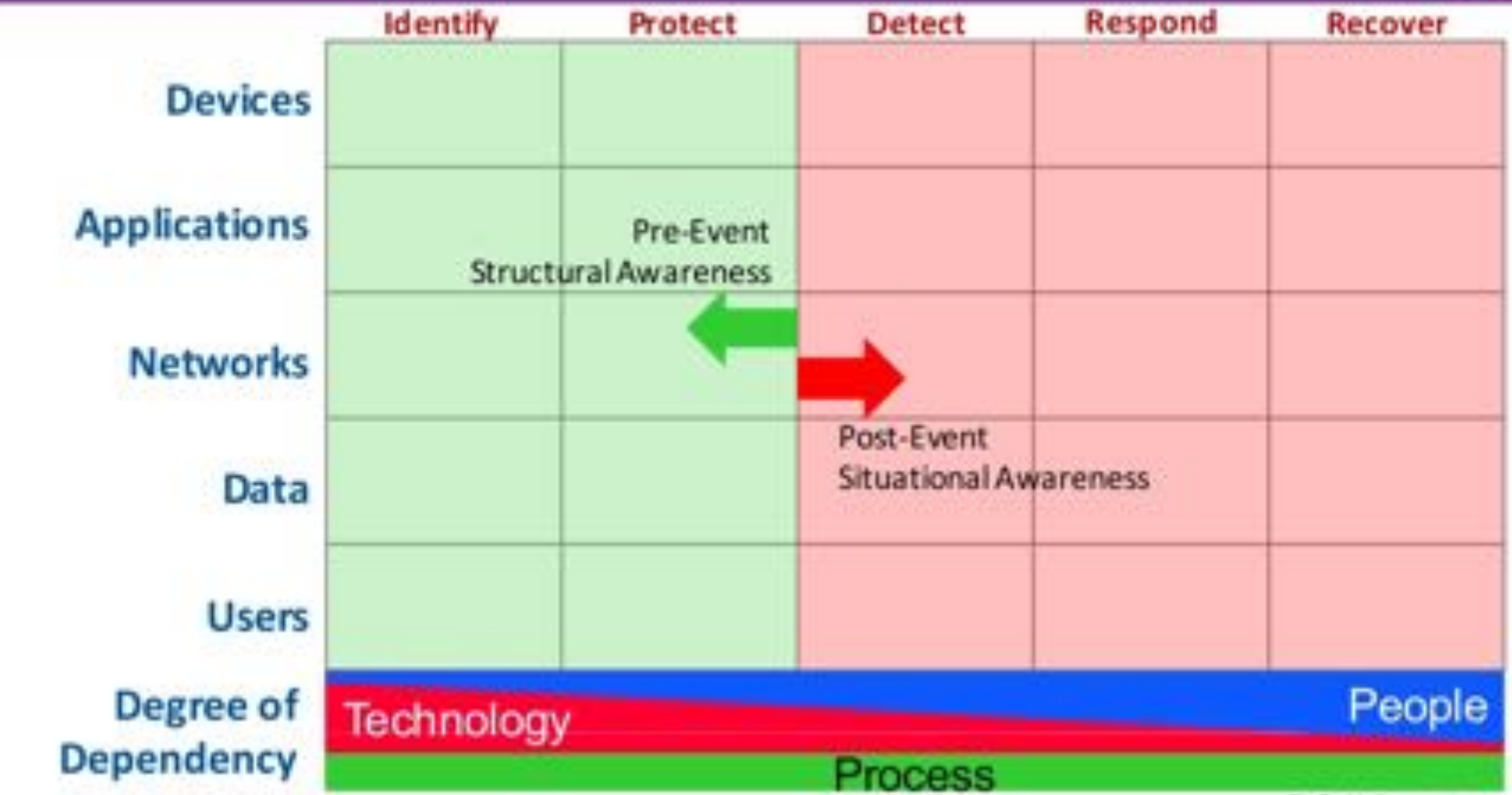
1. Attacker's Exploit Succeeds

Reality

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

Left and Right of "Boom"

Sounil Yu - right of boom



Introducing the "Cyber Defense Matrix"

Sounil Yu - matrix

#RSAC

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

Degree of Dependency: Technology, People, Process

Page Discussion

OWASP Cyber Defense Matrix

Main | FAQs | Roadmap | Contributors | Events and Opportunities to Get Involved

Donate

Introduction to the Cyber Defense Matrix

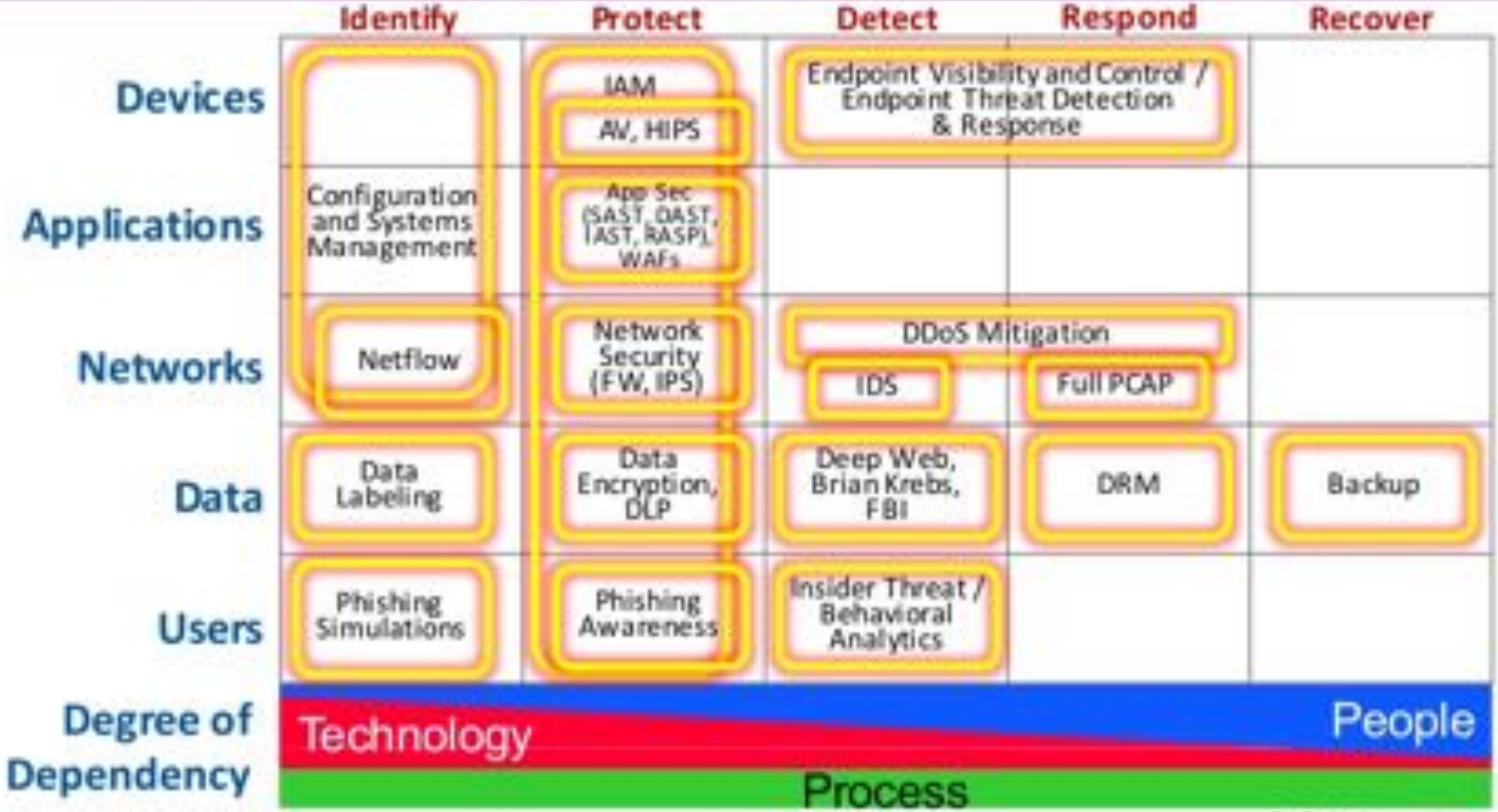
Imagine going into a grocery store to shop for Thanksgiving dinner, but instead of seeing nice, orderly aisles, you see a massive pile of food in the middle of the grocery store. Finding the ingredients that you need to make dinner is going to be extremely hard because there's no organizational system helping you understand where things are. The disorganization makes it very difficult to find what you need and compare competing products.

The cybersecurity vendor marketplace is like this disorganized grocery store. A proof of this assertion can be seen by looking at the vendor hall at any major security conference. The cacophony of sounds from vendors hawking their wares, the confusing language of the vendor's marketecture, and the lack of any semblance of organization (aside from biggest to smallest) does not help buyers understand what they need or where to find it.

Home
About OWASP
Acknowledgements
Advertising
AppSec Events
Supporting Partners
Books
Brand Resources
Chapters
Donate to OWASP
Downloads
Funding
Governance
Initiatives
Mailing Lists
Membership
Merchandise
Presentations
Press
Projects
Video

Reference
Activities
Attacks
Code Snippets

Enterprise Security Market Segments



Security Technologies Mapped by Asset Class

DEVICES
Workstations, servers, VoIP phones, tablets, IoT, storage, network devices, infrastructure, etc.

APPS
The software, interactions, and application flows on the devices

NETWORKS
The connections and traffic flowing among devices and applications

DATA
The information residing on, traveling through, or processed by the resources above

USERS
The people using the resources listed above

Disclaimer: Vendors shown are representative only. No usage or endorsement should be construed because they are shown here.

Security Technologies Mapped by Operational Functions

IDENTIFY	Inventorying assets, measuring attack surface, baselining normal, risk profiling
PROTECT	Preventing or limiting impact, containing, hardening, managing access
DETECT	Discovering events, triggering on anomalies, hunting for intrusions
RESPOND	Acting on events, eradicating intrusion footholds, assessing damage, coordinating, reconstructing events forensically
RECOVER	Returning to normal operations, restoring services, documenting lessons learned

TANIUM, Vorametrix, BITSIGHT, Tripwire, TITUS, THREATSTREAM, DOMAINTOOLS, skyhigh, Lancope, BIOCATCH, ThreatMetrix, ForeScout, comilion, ARBOR, CROWDSTRIKE, FARSIGHT SECURITY, DataGravity

AUTHENTIFY, VERACODE, ARXAN, BLUE COAT, waratek, Security Compass, Symantec, CYLANCE, CONTRAST, skyhigh, zscaler, CipherCloud, SafeNet, PHISHME, NowSecure, Voltage, invincea, cigital, Malwarebytes, Bit9+CARBON BLACK, CHECKMARX, INTRALINKS, CYBERARK

Lancope, Tripwire, TANIUM, Lastline, SECURONIX, ZEROFOX, ARBOR, Dtex, FIDELIS, FORCEPOINT, TRIUMFANT, exabeam, CYPHORT

Bit9+CARBON BLACK, TANIUM, BLUE COAT, NowSecure, TRIUMFANT, RSA

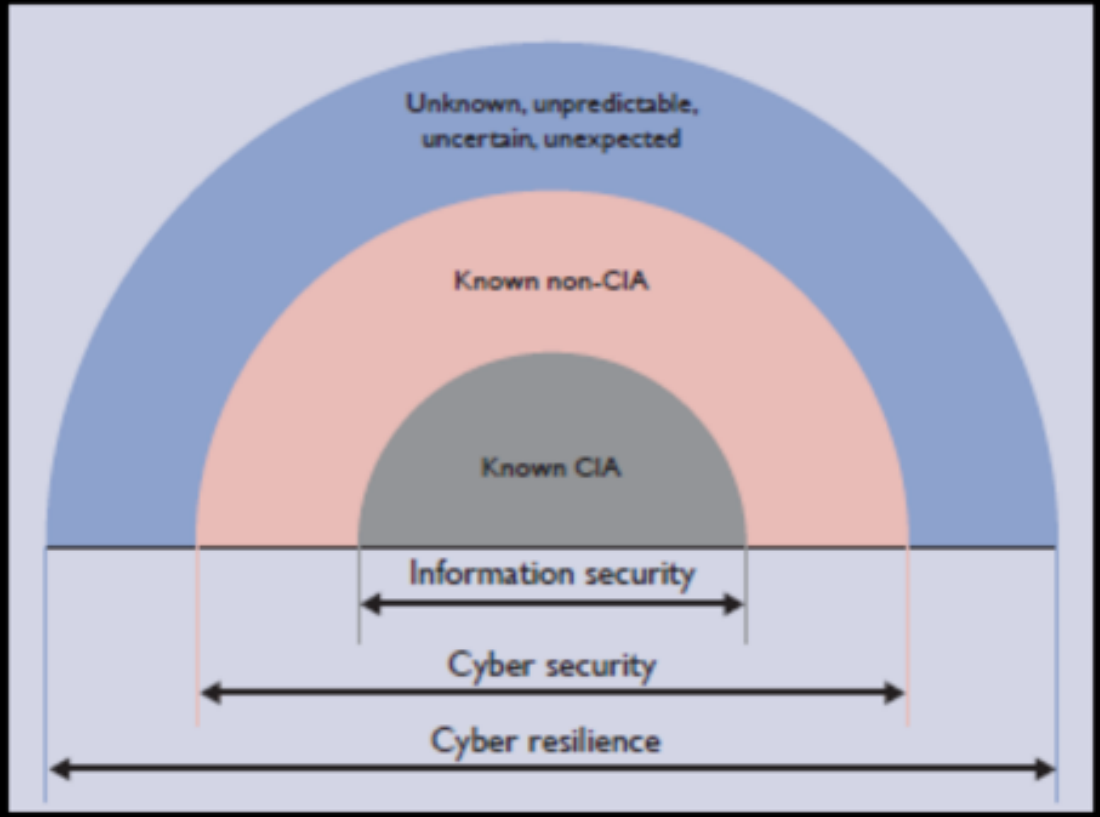
MSSPs / IR: Deloitte, PwC, EY, accenture

VERITAS

Disclaimer: Vendors shown are representative only. No usage or endorsement should be construed because they are shown here.

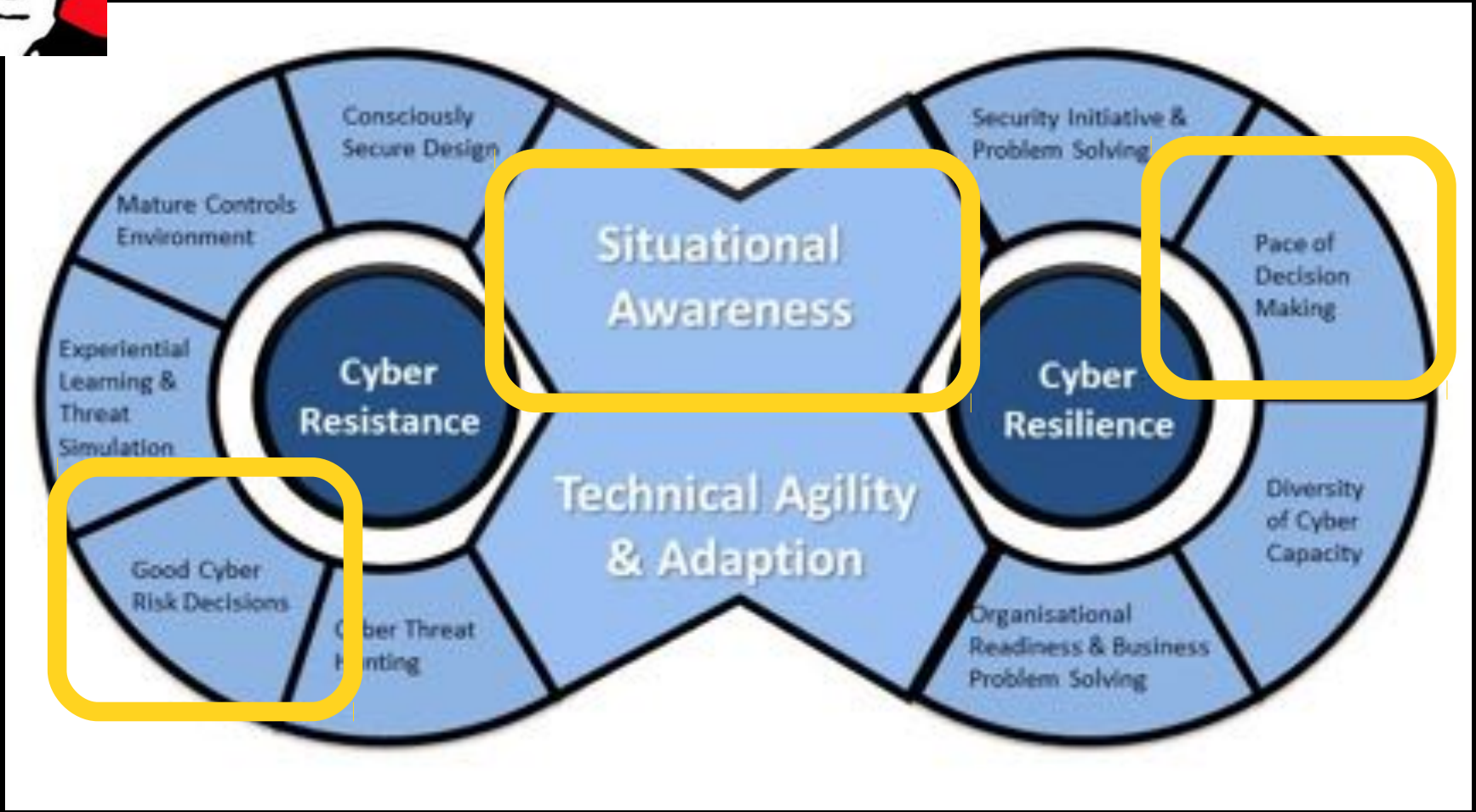
Security Technologies by Asset Classes & Operational Functions

We are meant to be resilient now



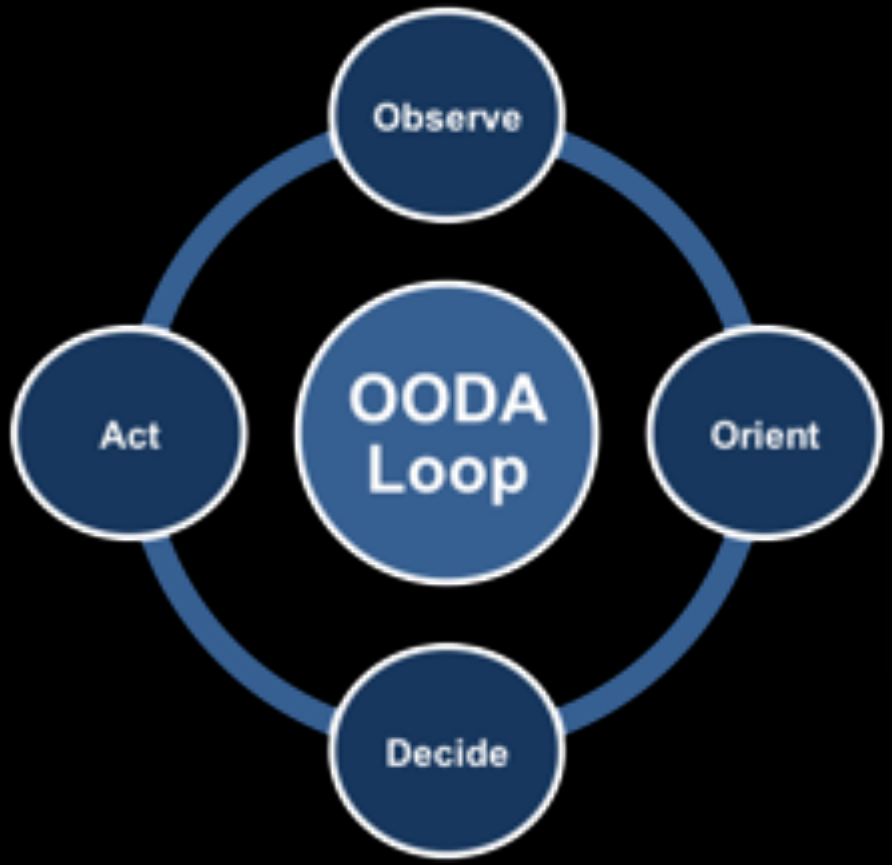
Source: ISF - Cyber Security Strategies

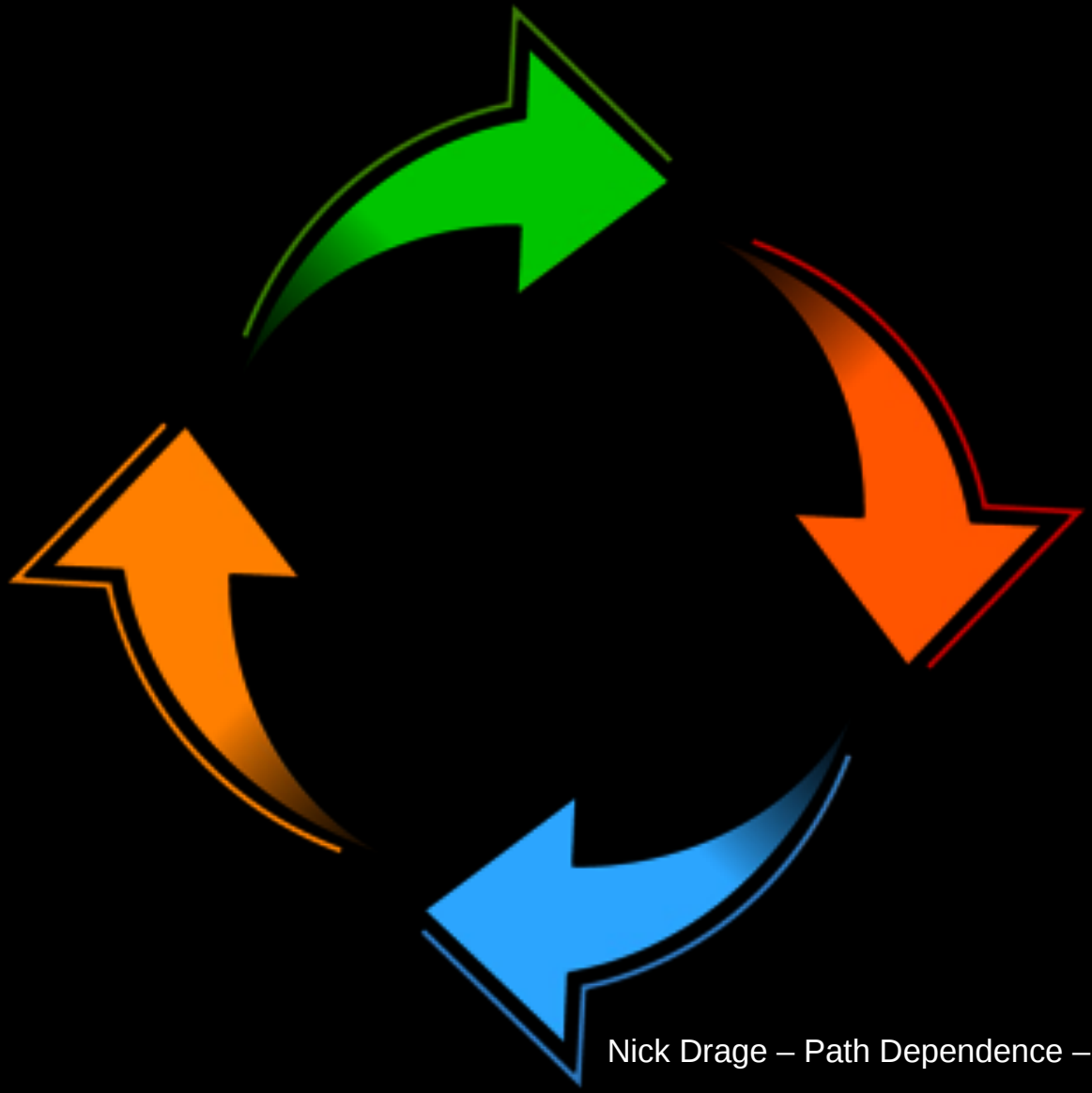
Blog - Black Swan Security

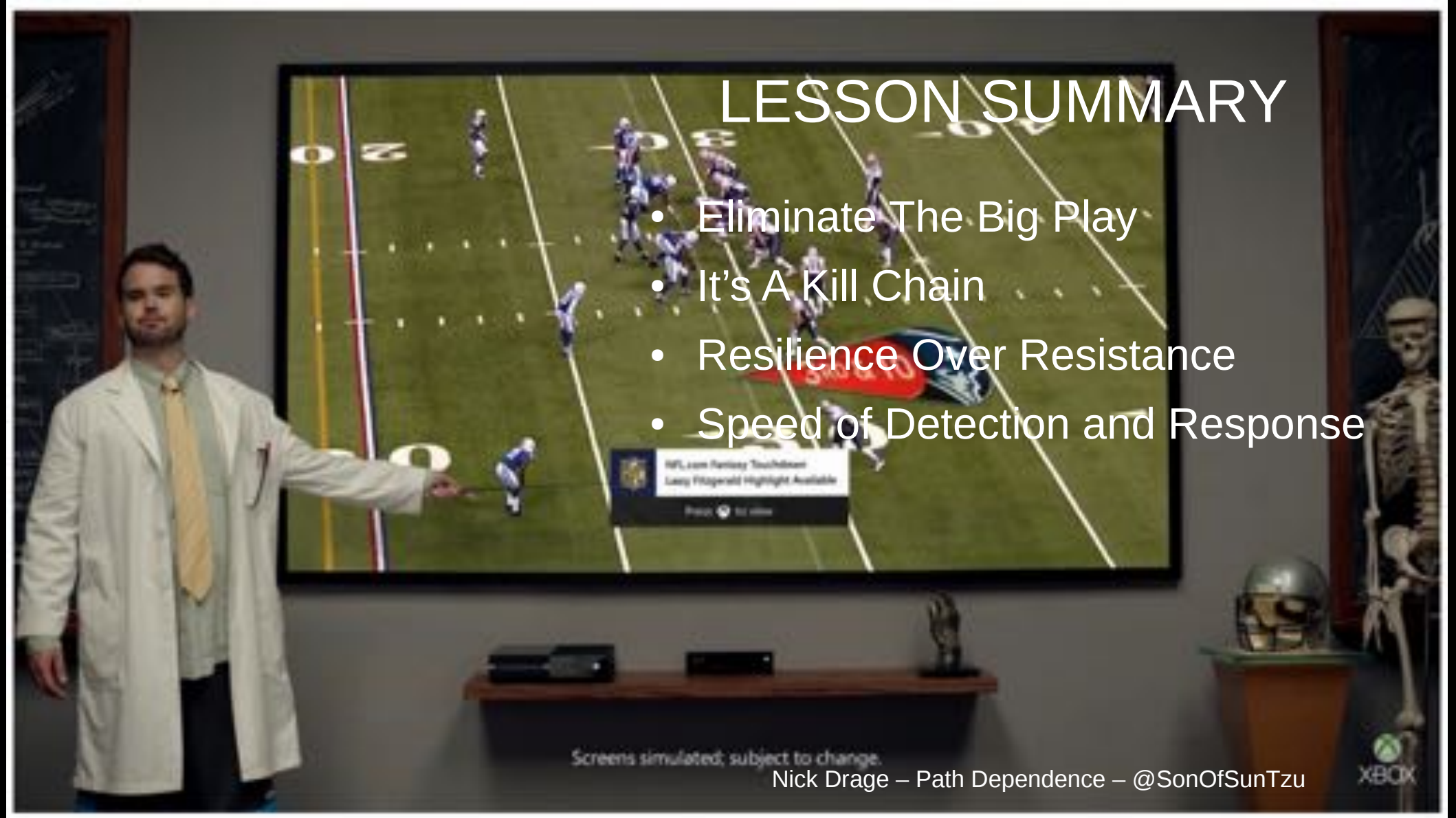


Colonel John Boyd - USAF

OODA: Observe – Orient – Decide - Act

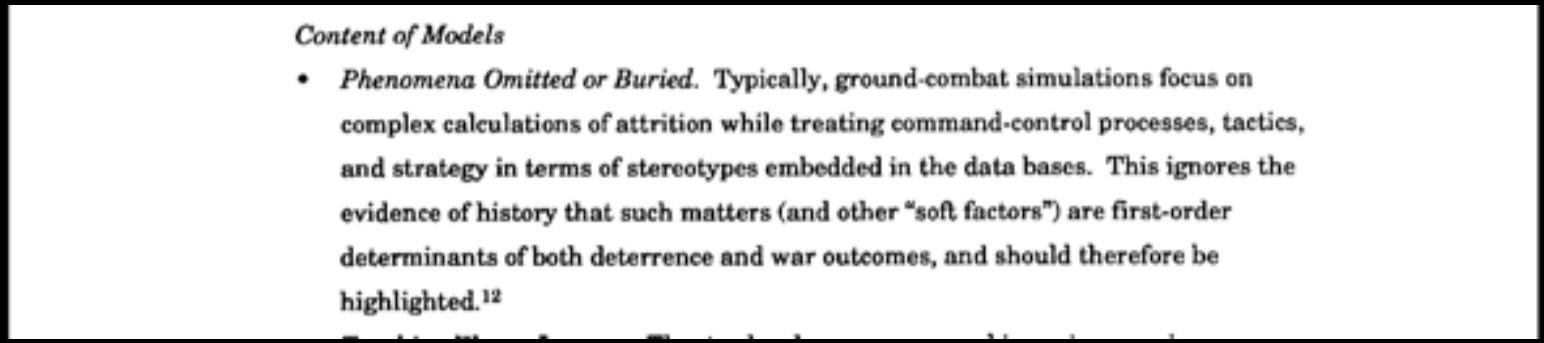





LESSON SUMMARY
• Eliminate The Big Play
• It's A Kill Chain
• Resilience Over Resistance
• Speed of Detection and Response
Screens simulated; subject to change.
XBOX

LESSON – Out Hit Your Opponent

The Base Of Sand Problem



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

Nick Drage – Path Dependence – @SonOfSunTzu

Nick Drage – Path Dependence – @SonOfSunTzu

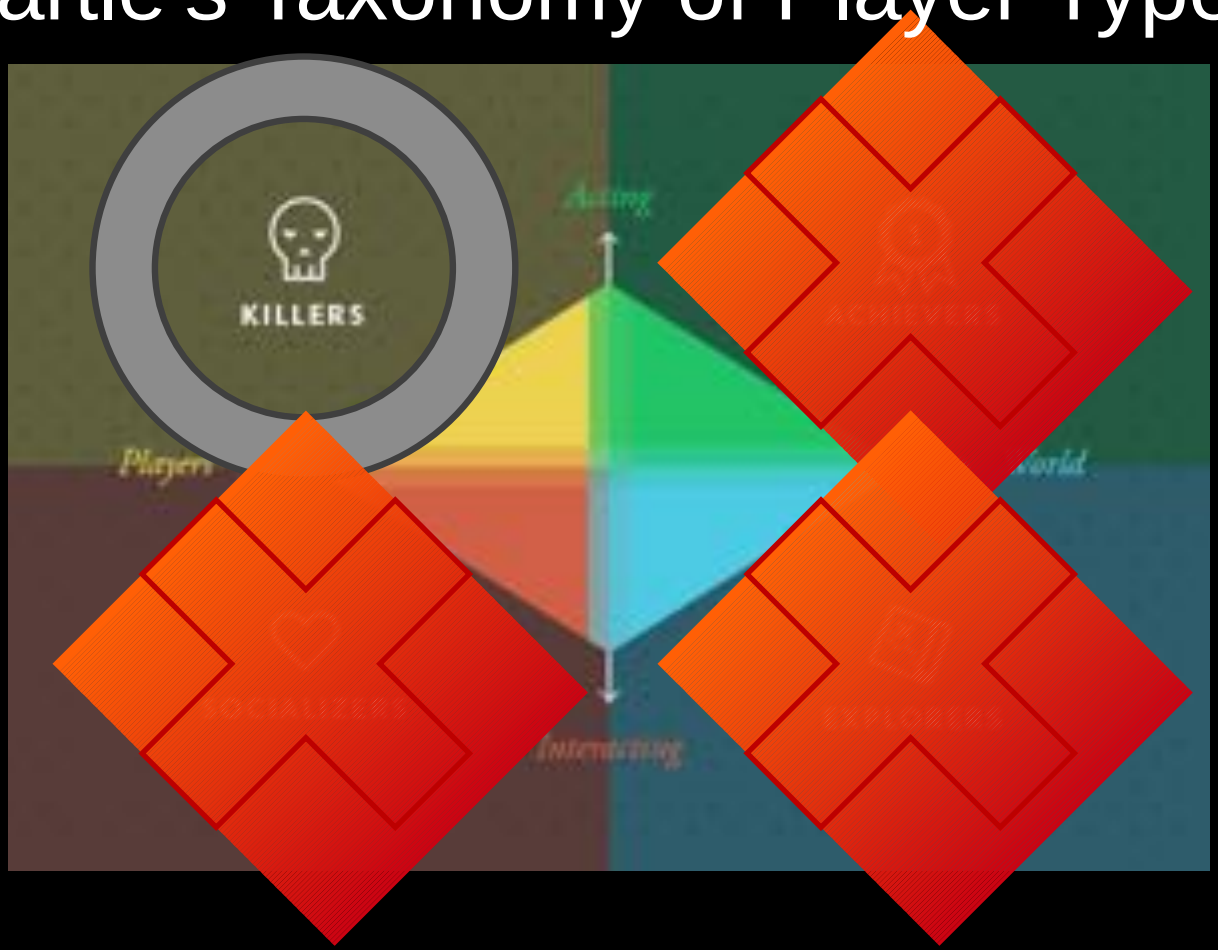
What made the LOB horrifying … a blend of belligerence and violence unmatched in its era

Gold / Silver / Bronze

GOLD	STRATEGIC
SILVER	TACTICAL
BRONZE	OPERATIONAL

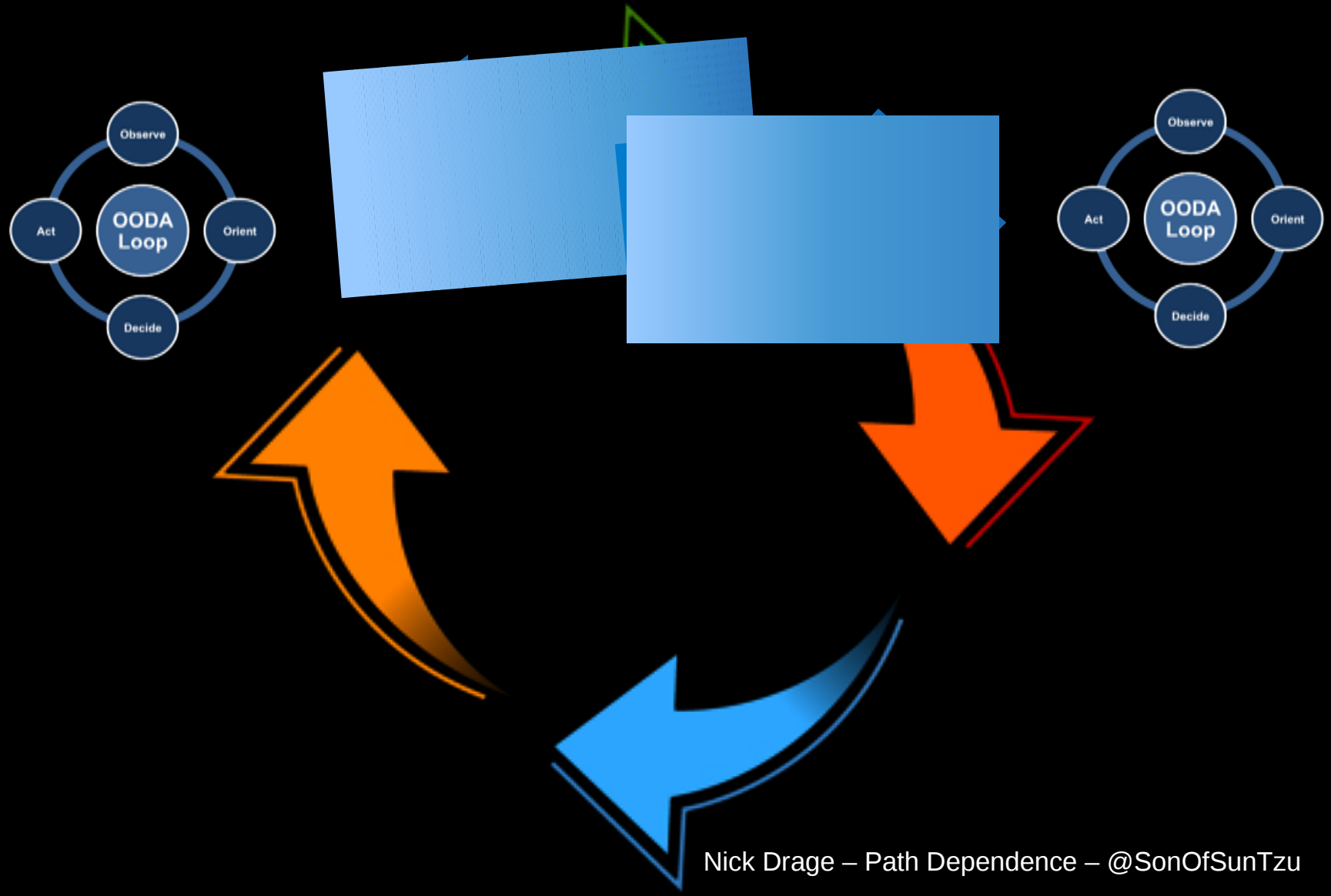
Image: Towyn and Kinmel Bay Flood Planning - yourbiz.org

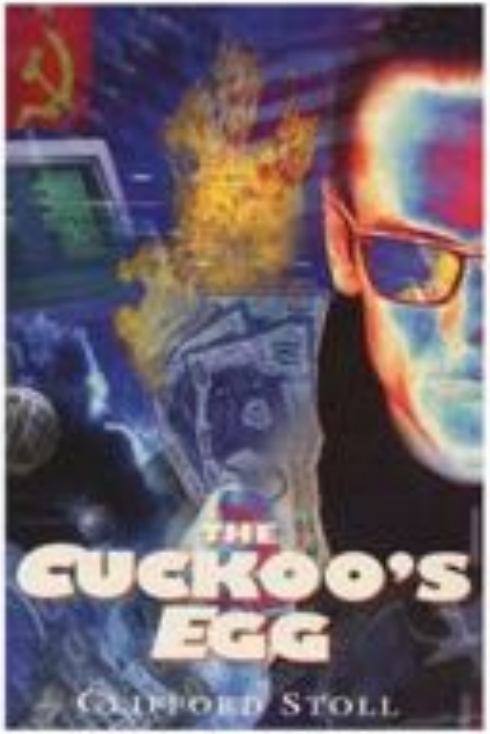
Bartle’s Taxonomy of Player Types



Nullcon Goa 2018:- Keynote by Haroon Meer

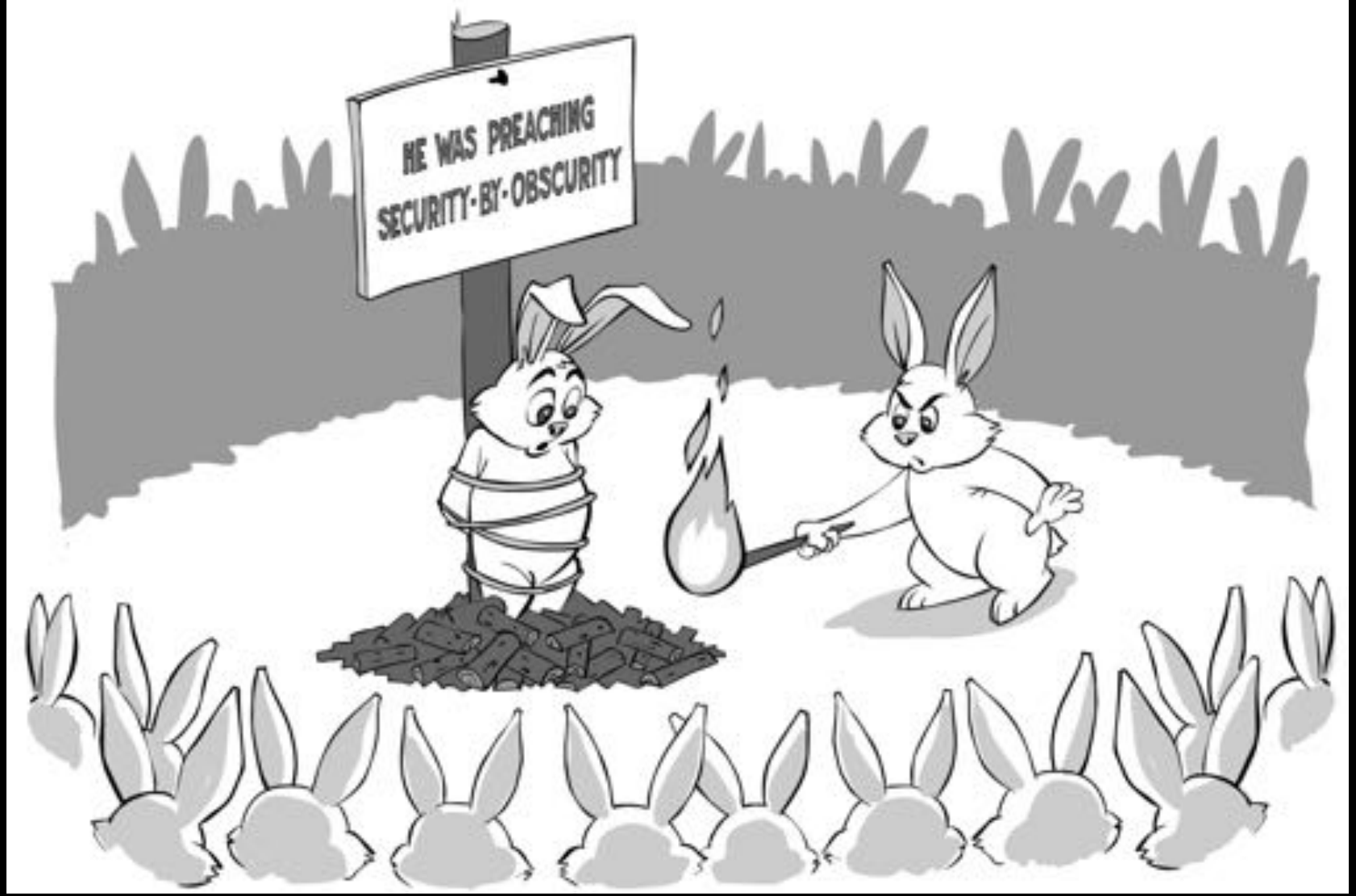
Image: Yan Cui


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



Everyhing You Know Is Wrong - Paul Midian

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


HE WAS PREACHING
SECURITY-BY-OBSCURITY

Keynote: The Seven Axioms of Security


Seven Axioms of Security: 6
The Best Defense
is a CREATIVE
Defense.

Image: Meadow Ellis

Image: DevSecCon

Agenda

- What do I mean "Attack Aware Applications?"
- Where has the idea come from?
- What is happening in this space?
- What can ***you*** do with this?
- Future thoughts

AppSensor | Home | Overview | Getting Started | User Guide | Documentation | API | OWASP

AppSensor

Real-time event detection, analysis and response

The Idea

The AppSensor project defines a conceptual framework and methodology that offers prescriptive guidance to implement application intrusion detection and automated response.

(The documentation is under a Creative Commons Attribution-ShareAlike 3.0 open-source license.)

Current Version: 2.0.1

Learn more »

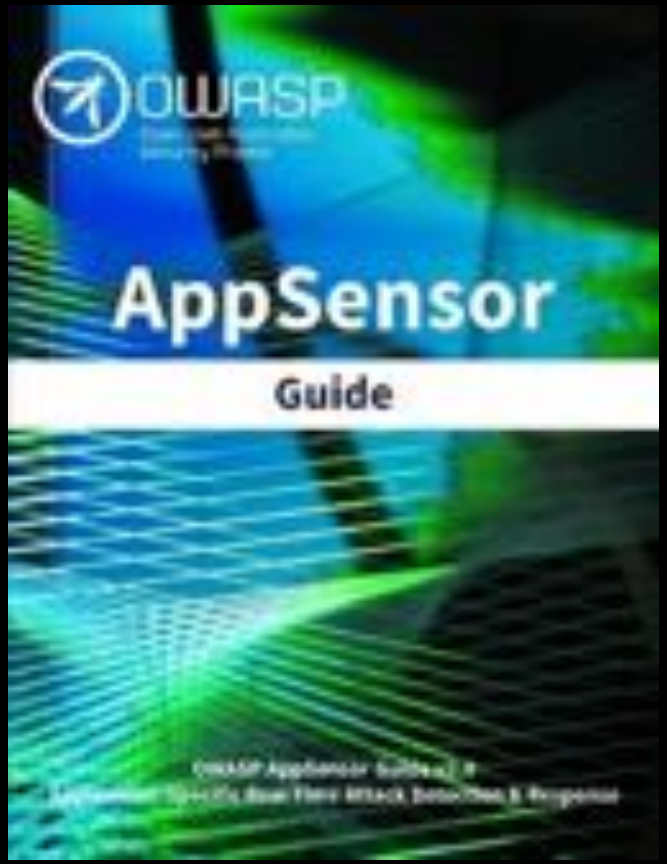
The Tool

In addition, the project also provides a reference implementation that allows developers to use these powerful concepts in existing applications.

(The tool is under an MIT open-source license.)

Current Versions: 2.3.1 (SNAPSHOT) and 2.3.1 (release)

Get Started »



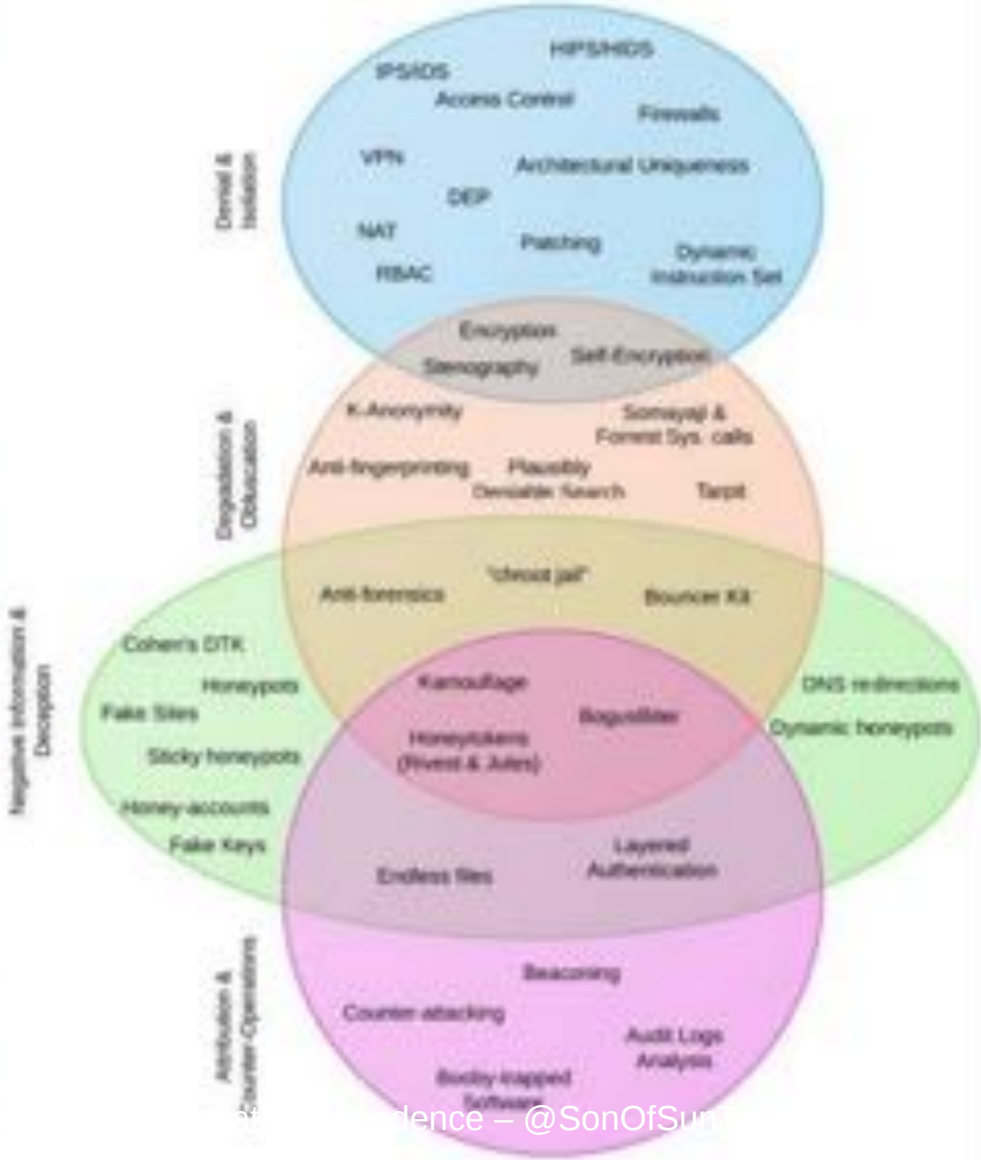
Nick Drage – Path Dependence – @SonOfSunTzu

Nick Drage – Path Dependence – @SonOfSunTzu

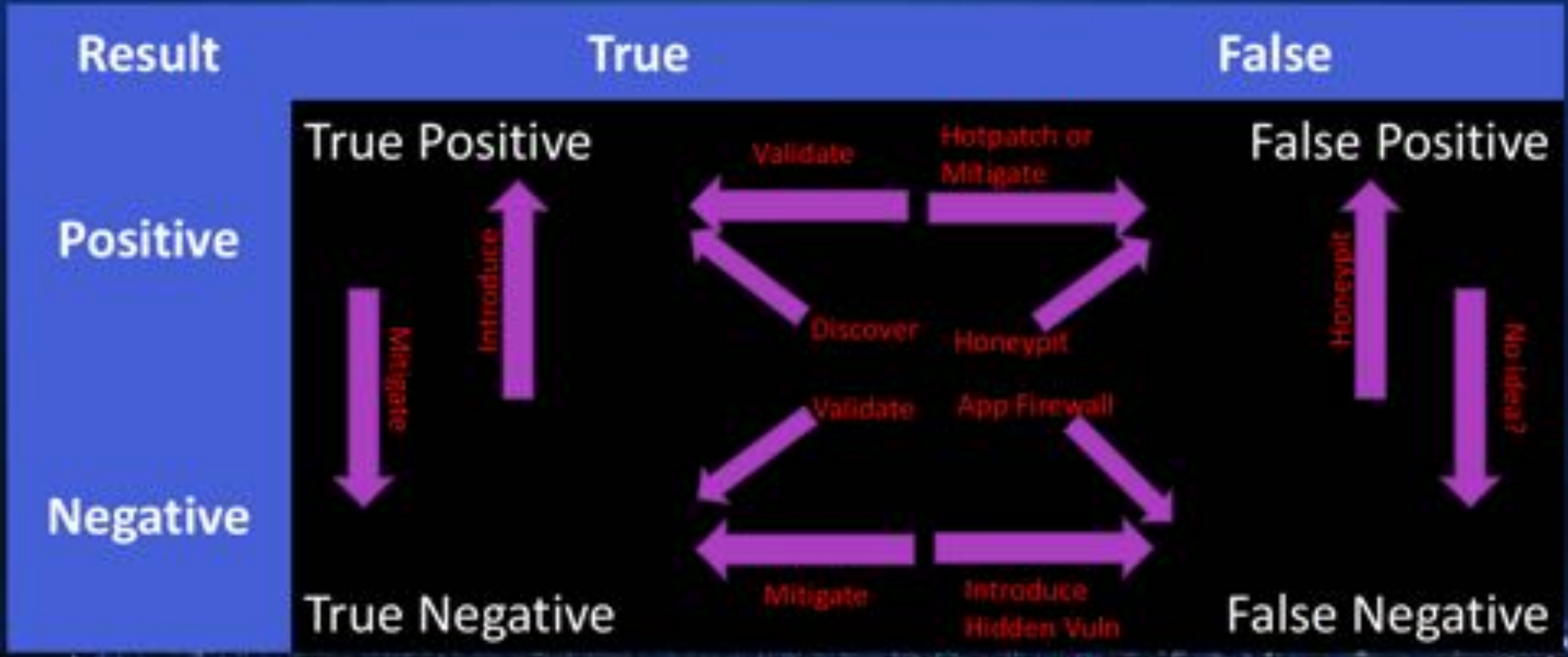

"Never attempt to win by force what can be won by deception."
Niccolò Machiavelli,
The Prince

DECEPTION EXAMPLES – INFORMATION SECURITY

- From Almeshekah



POSSIBILTIES - TRANSITIONS



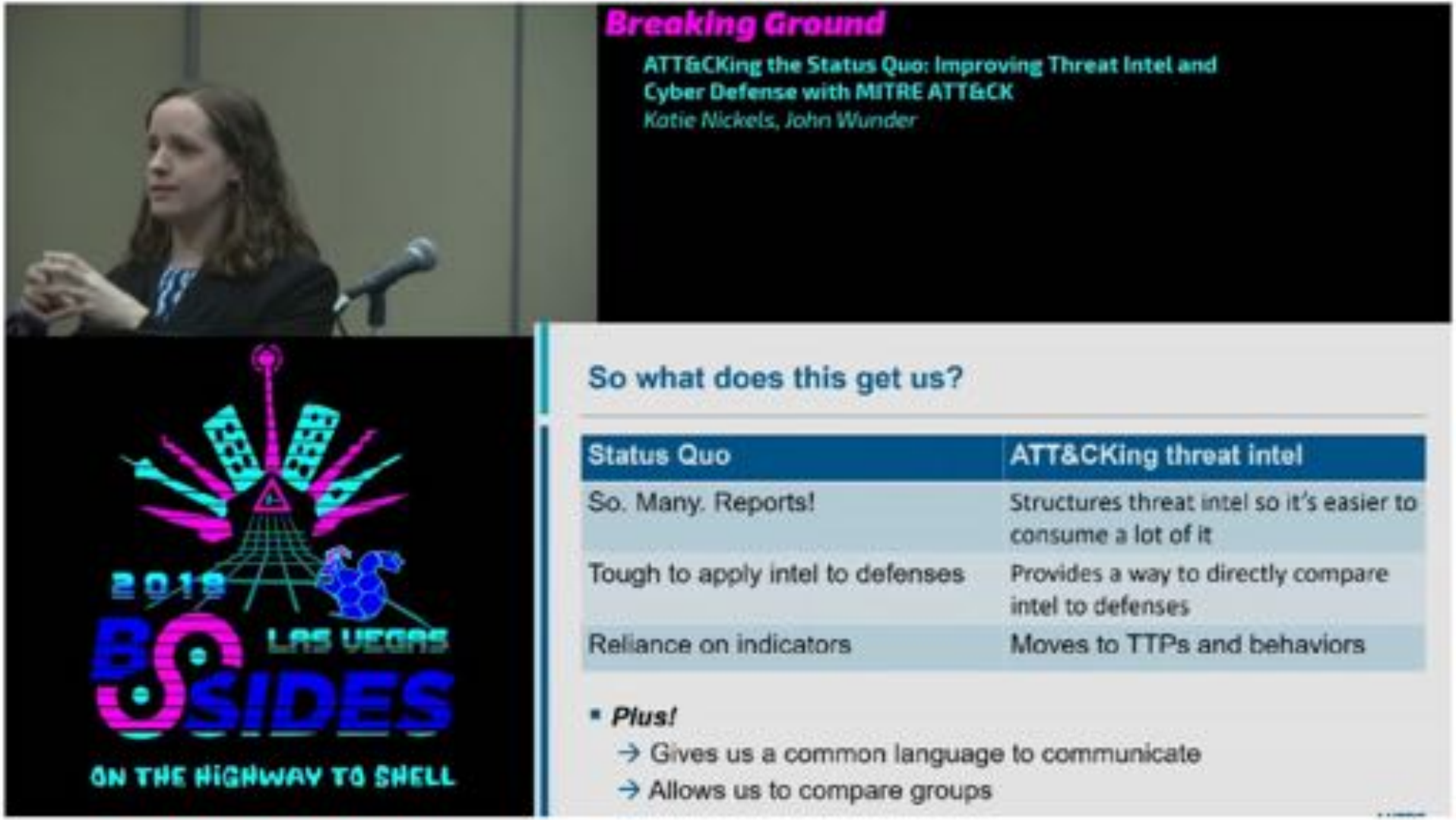
TRANSIENT PROBLEMS – MISSPEAKING

ANSWER PRETTY MUCH AS EXPECTED BUT NOT QUITE

- Random errors
  - Random timing errors
  - Random omissions
  - Random bitflips
  - Random endian changes
  - Random number changes
  - Badly signed things
  - Badly encrypted things
  - Random wrong content
- Nonrandom errors to break things
  - Invalid characters/bytes
  - Terminal command characters
  - Random "unallocated" memory
  - Bad pointer values
  - Filesystems of the wrong type
  - Impossible filenames
  - Timing "errors"
  - "Omissions"

GASLIGHTING - MORE

- Uncrackable Hashes
- Decoy Systems, Ports, Services
- Manufactured Vuln Emulation
  - E.g. MS08-067?
- Decoy Vulns (static)
- Decoy Vulns (non exploitable {buffer overflow in managed lang})
- Nondeterministic Existence
- For you only existence
- Transient Vulns
- Transient Systems, Ports, Services
- Vuln neutering
- Vuln Chains leading nowhere
- Benign Passthrough
- Honeypot Passthrough
- Trickster passthrough
- One time Vulnerability Generation
- One time vulns as canaries
- Answering questions you never asked
- Answering different questions
- Fake answers
- Fake Data
- Silent Failure (denying you ever agreed)
- Rewriting page format dynamically to break validation and cscripting



BG - ATT&CKing the Status Quo: Improving Threat Intel and Cyber Defense with MITRE ATT&CK - Katie Ni

So what does this get us?

Status Quo	ATT&CKing threat intel
So. Many. Reports!	Structures threat intel so it's easier to consume a lot of it
Tough to apply intel to defenses	Provides a way to directly compare intel to defenses
Reliance on indicators	Moves to TTPs and behaviors

- ***Plus!***
  - → Gives us a common language to communicate
  - → Allows us to compare groups

Solving Threat Detection - Alex Davies

Nick Drage – Path Dependence – @SonOfSunTzu

Defender's Dilemma

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

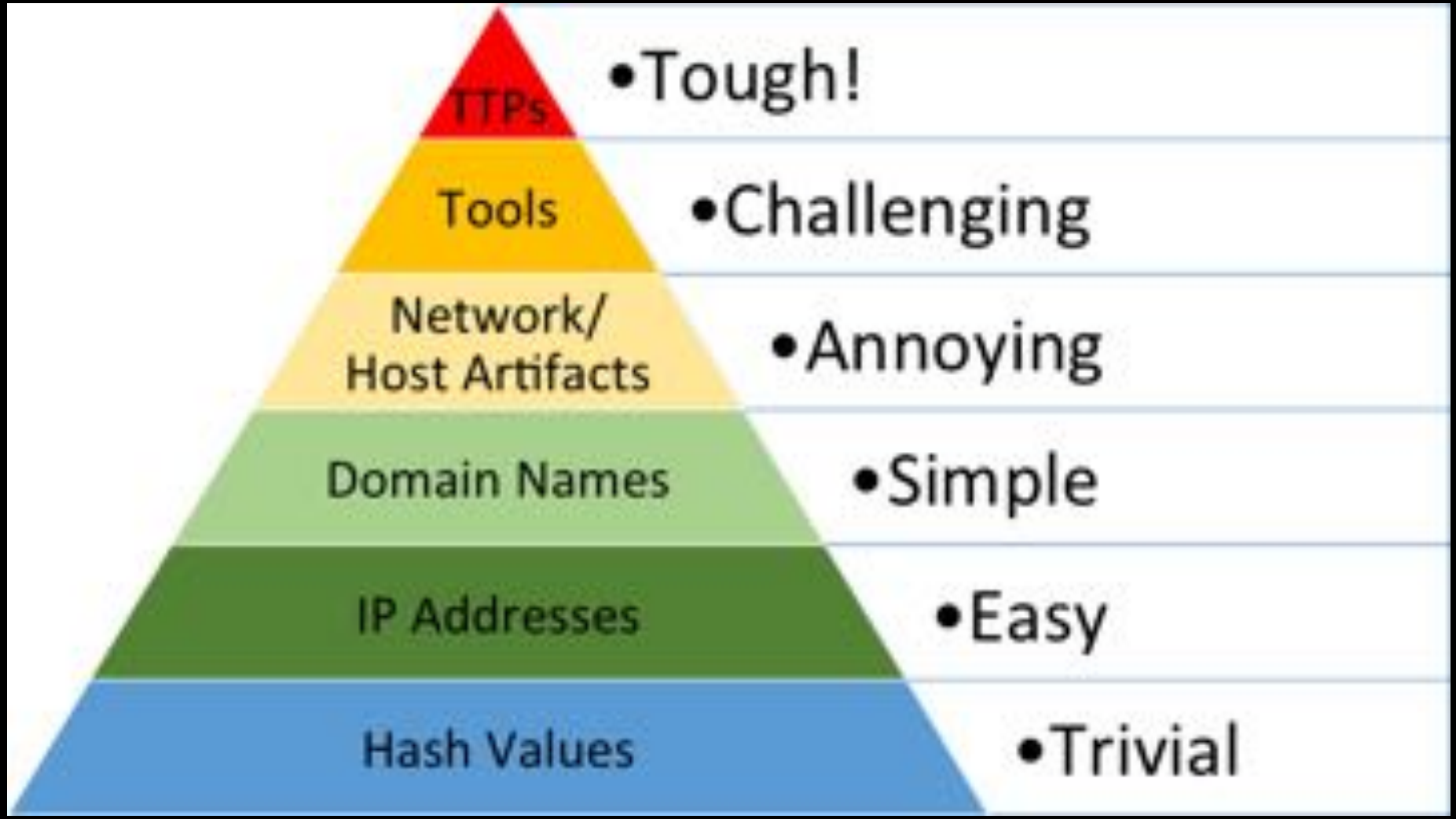
Intruder's Dilemma

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

Nick Drage – Path Dependence – @SonOfSunTzu


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

CHANGE CONTROL?

“The Scream” by Edvard Munch

Image: @OWASP_NL

RSAConference2017

San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: MASH-F02

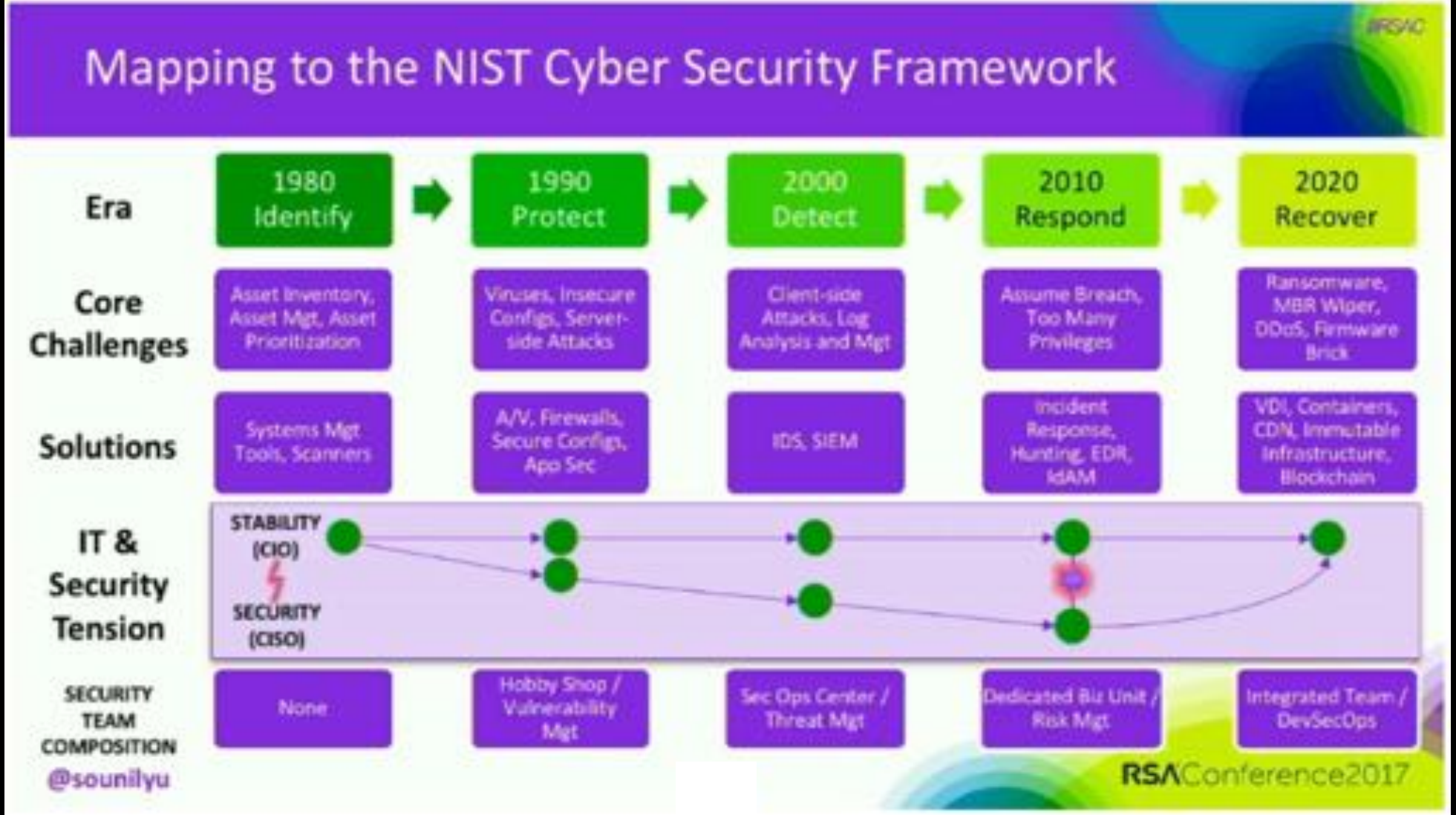
Solving Cybersecurity in the Next Five Years

Systematizing Progress for the Short Term

Sounil Yu

@sounilyu

Solving Cybersecurity in the Next Five Years: Systematizing Progress for the Short Term

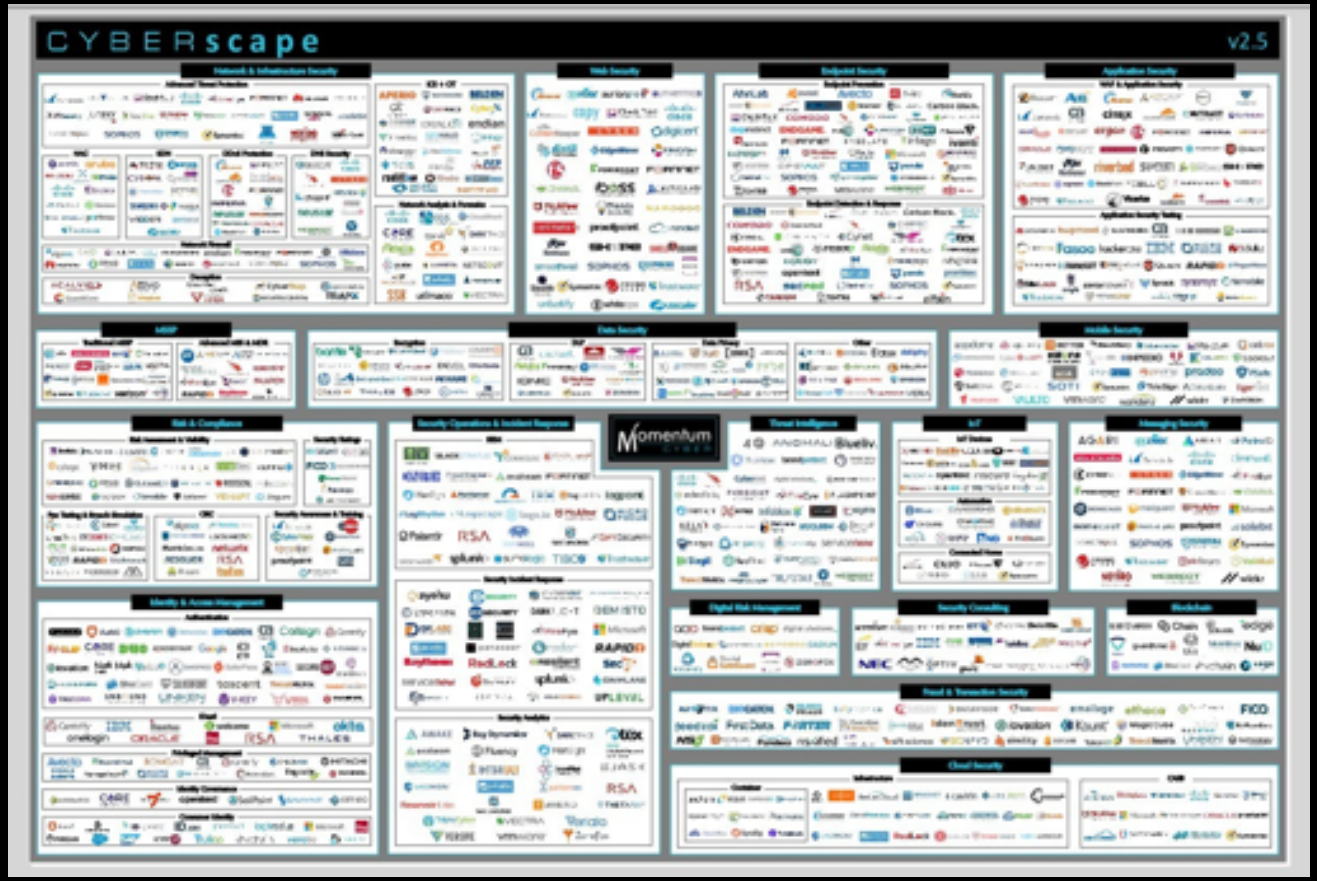


Solving Cybersecurity in the Next Five Years: Systematizing Progress for the Short Term

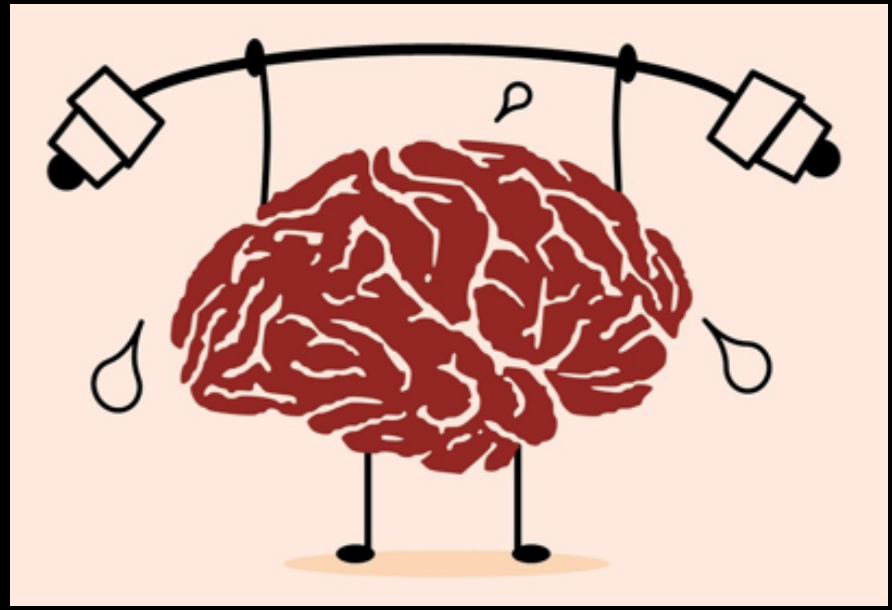
Not a blinky box you can buy, install and ignore

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

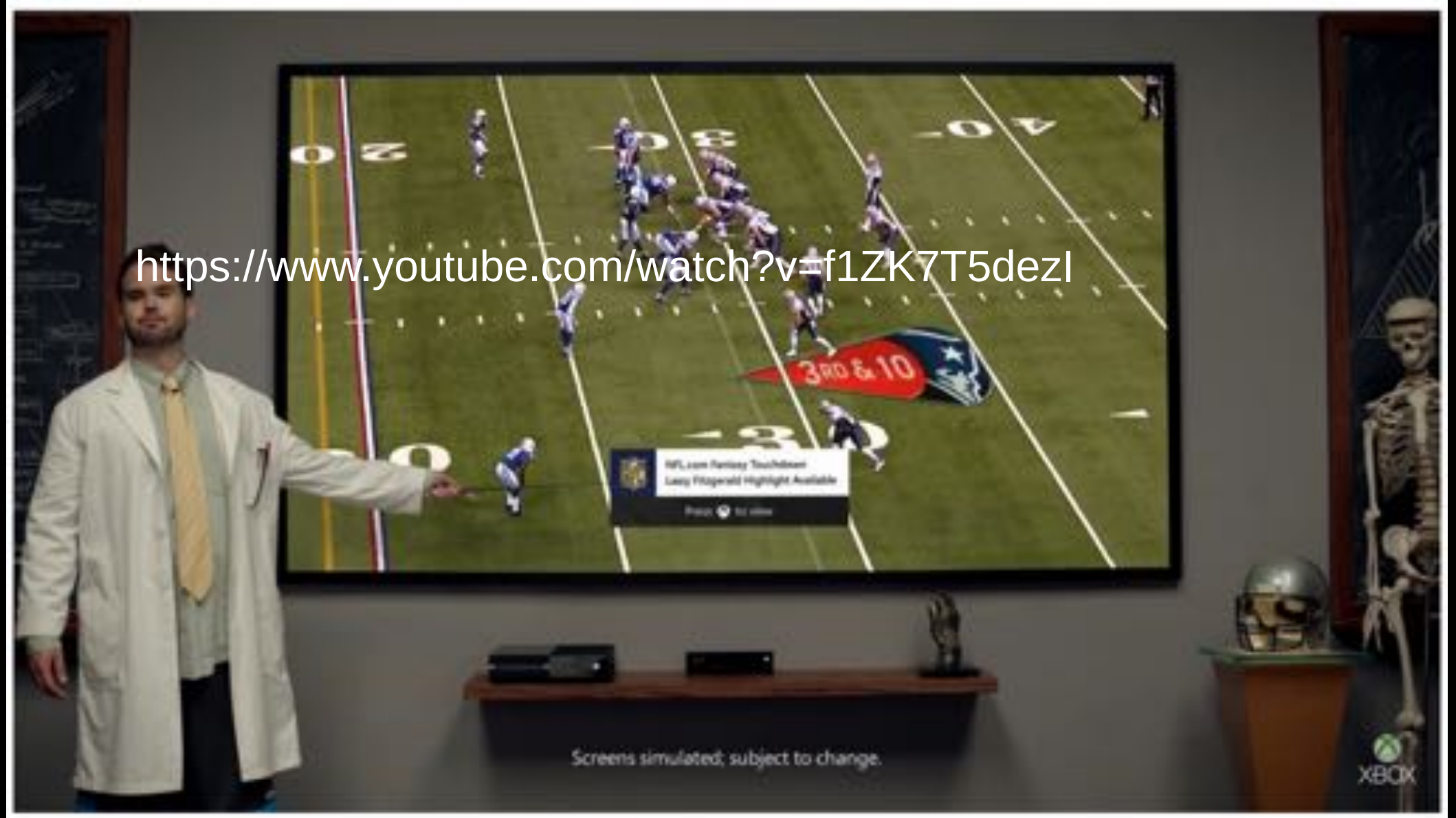
“peak security product”



Nick Drage – Path Dependence – @SonOfSunTzu




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


https://www.youtube.com/watch?v=f1ZK7T5dezI
3RD & 10
Screens simulated; subject to change.
XBOX


LESSONS
• Use others' lessons
• Practice Is Everything
• Eliminate the Big Play
• Out Hit Your Opponent
• Or try to Golf our way through American Football...
Screens simulated; subject to change.
XBOX

Nick Drage – Path Dependence – @SonOfSunTzu

Nick Drage

Email: **nickd@pathdependence.co.uk**
WWW: **blog.SonOfSunTzu.org.uk**
Twitter: **@SonOfSunTzu**