Cyber Essentialism

Security Discipline, Collective Defense and the Pursuit of Less

Ben Johnson I March 2017

v3.1

What is today’s goal?

TO SPARK CONTEMPLATION

(and give you something to remember!)

Quick Background Check

- Experience
  - **NSA | U.S. Defense & Intelligence**
    - Intrusion Operations Division
  - **Carbon Black**
    - Co-Founder & CTO
    - Wrote initial EDR product
    - Spoke to 600 Orgs, 500,000 miles
  - **Ten Eleven Ventures (VC)**
    - Executive in Residence
    - Launching a new security company soon!!
- Education
  - University of Chicago (C.S.)
  - Johns Hopkins University (C.S.)
- Connect: **@chicagoben | LinkedIn: benjaminjohnson80**

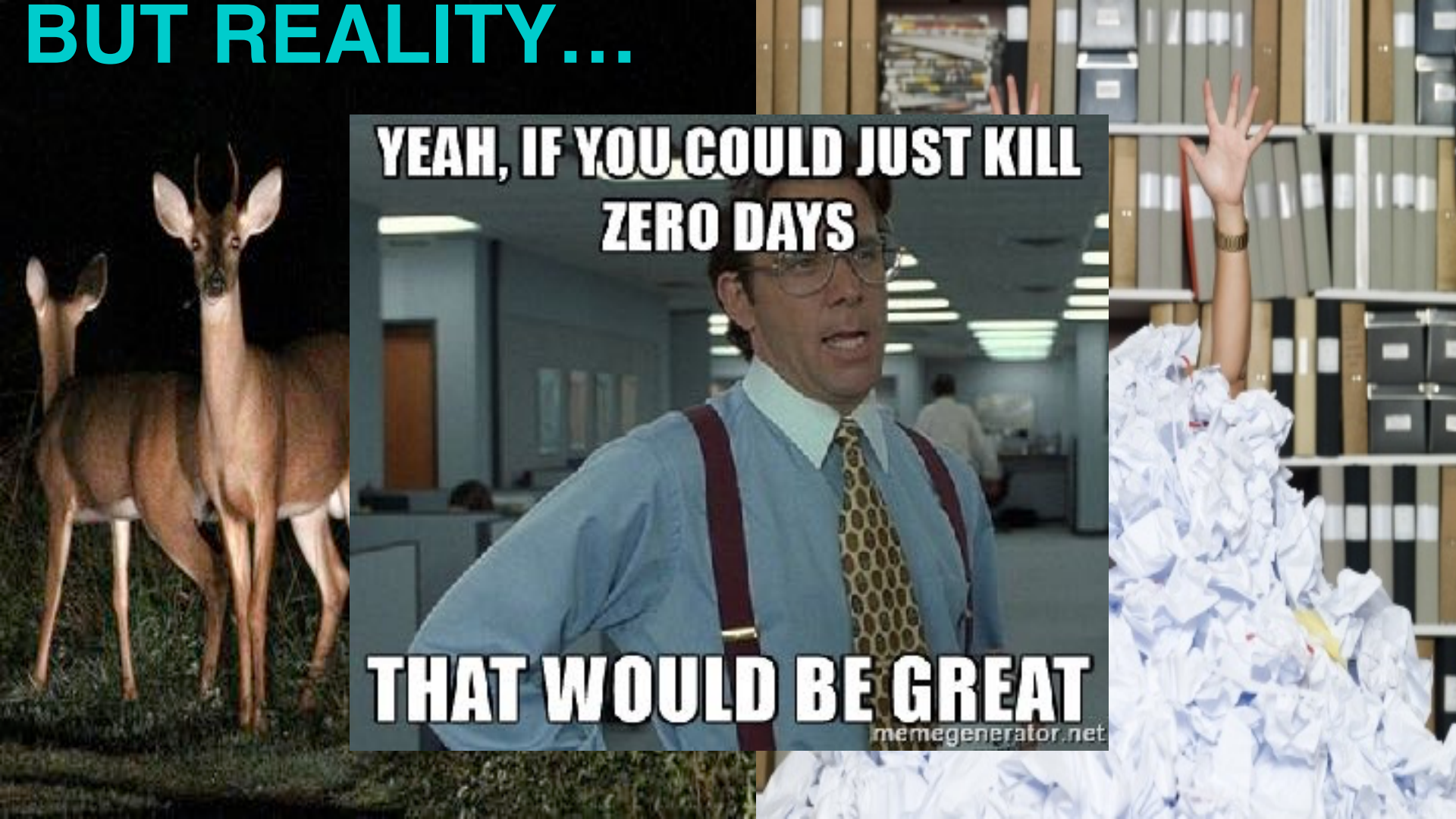
“**Efficiency** is doing **things right**;

Effectiveness is doing **right things**.”

– Peter Drucker, Business & Management Guru

ARE YOU AIMING FOR THIS?

BUT REALITY…


YEAH, IF YOU COULD JUST KILL ZERO DAYS
THAT WOULD BE GREAT
memegenerator.net

TOO MANY DISTRACTIONS

Architecture Review
Capturing Metrics
HR
Helpdesk Tickets
Tactics, Strategy & Ops
Bakeoffs
Meetings
RFPs
Troubleshooting
Recruiting
Reading Blogs


Essentialism?

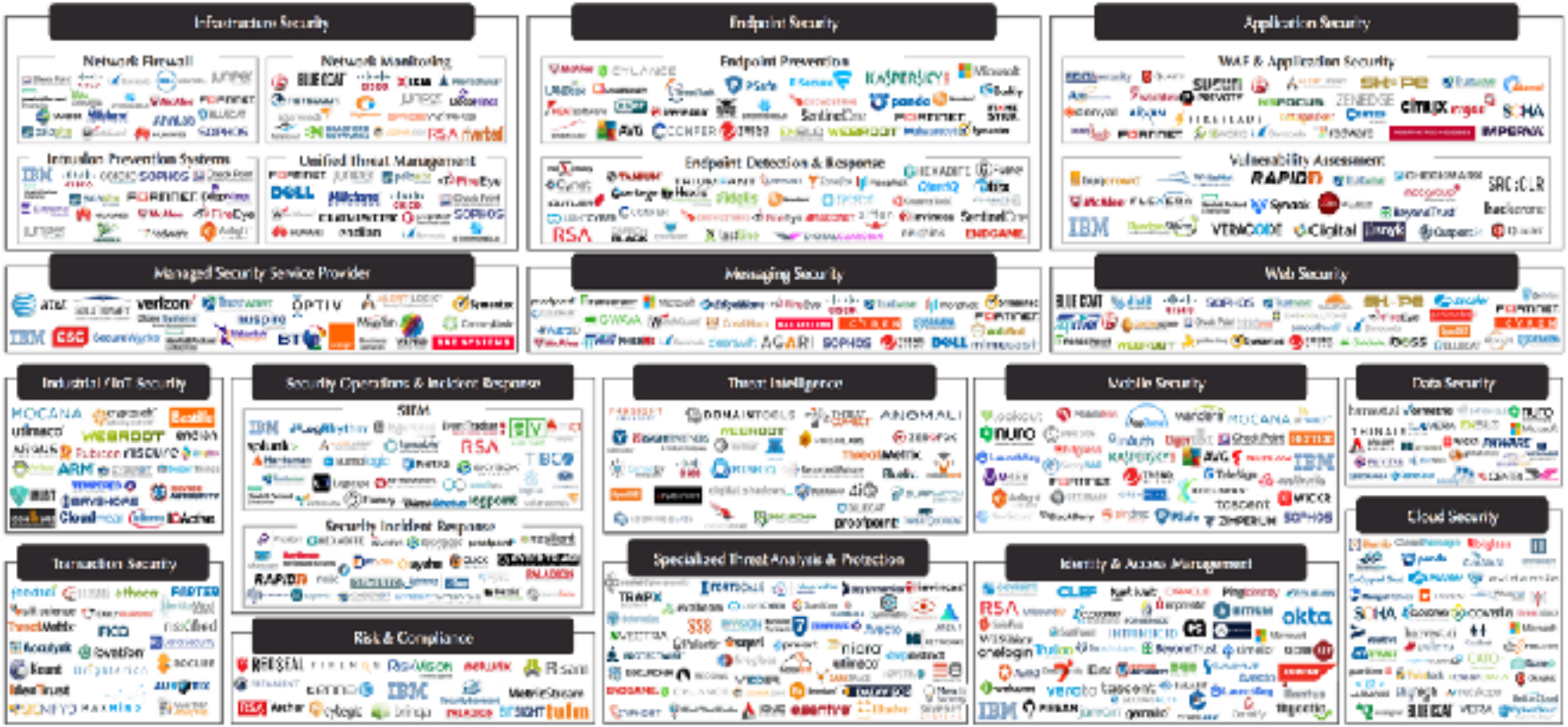
“It is about **making** the **wisest** possible **investment** of **your time** and energy in order to **operate** at our **highest** point of **contribution** by **doing** only what is **essential**.”

– *Greg McKeown, Author of Essentialism*

Rethinking Our Approach

CYBERscape: The Cybersecurity Landscape

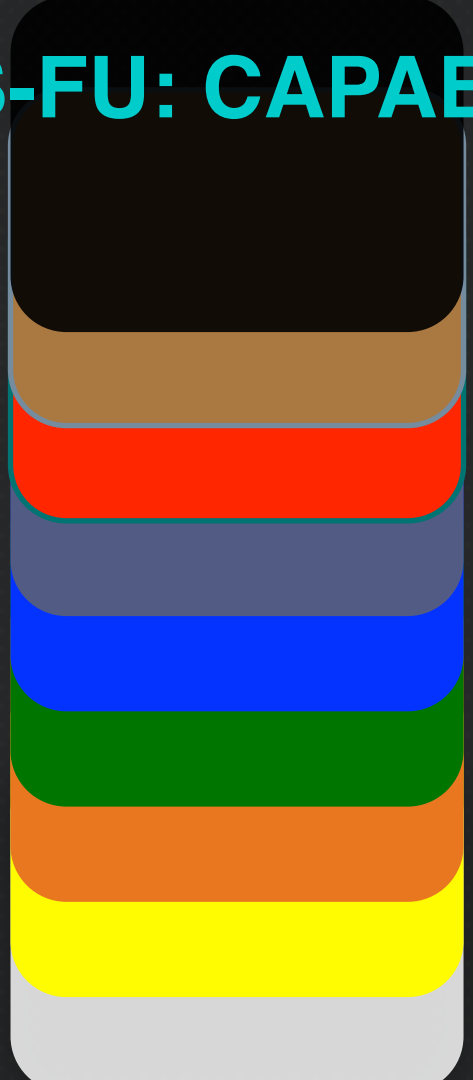
The Security Sector Is Dynamic And Vast. We Are Ceaseless & Vigilant In Our Coverage.



Source: Momentum Partners.

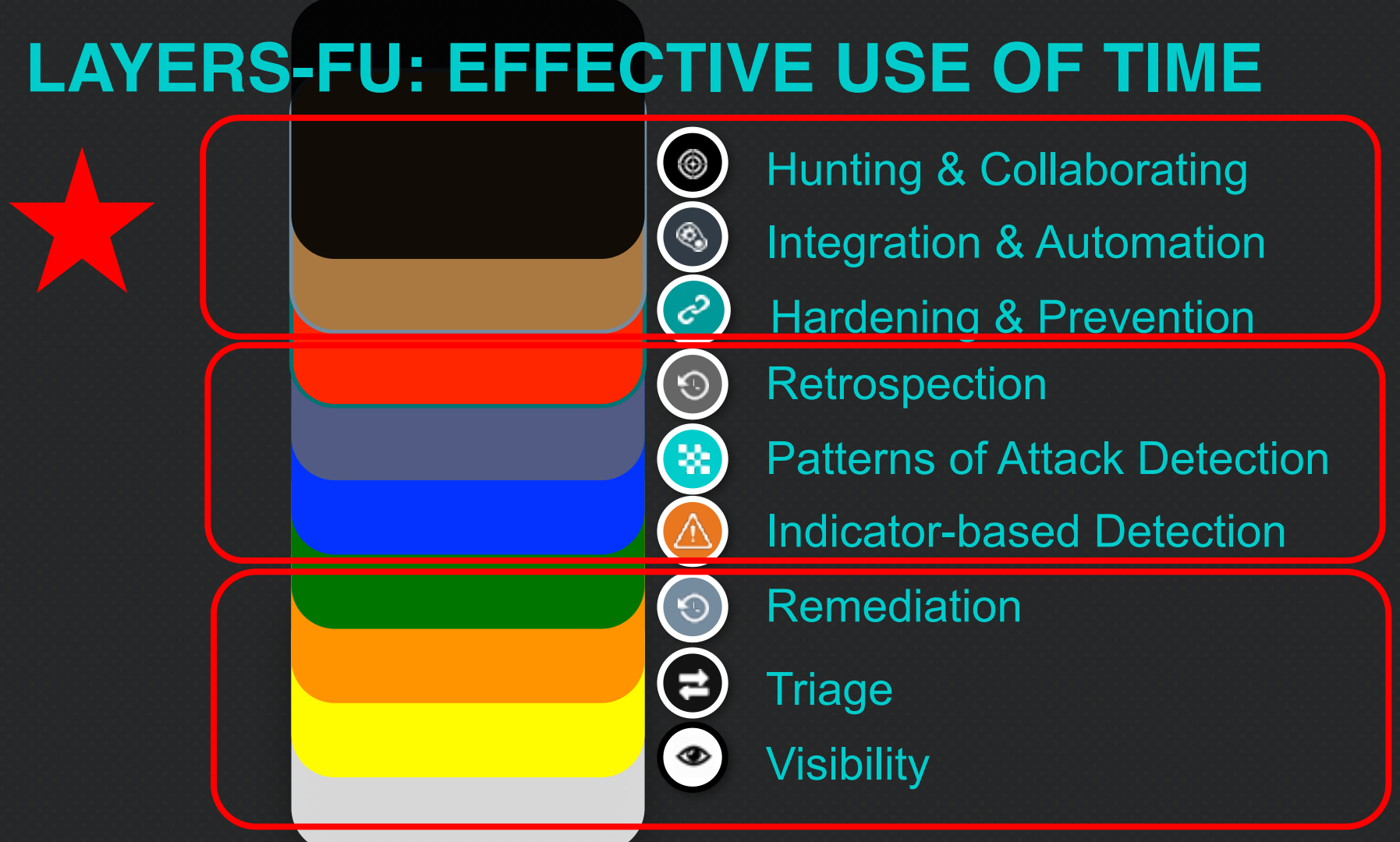

SERVER
DATA
PROXY
RESOURCE
COMPUTING
PERFORMANSE
AVAILABILITY
TYPE
HARDWARE
APPLICATION
NETWORK
DATA CENTER
GAMING
OPTIMIZATION
SYSTEM
CLIENT
RAID
RACK
MIGRATION
ARCHITECTURE
COMMUNICATION
CATALOG
BUSINESS
SERVICE
BACKUP
OPERATING SYSTEM
DESIGN
MAIL
SECURITY
SOFTWARE
FAX
PRINT
RESTORE
FAILURE
ADMINISTRATION
DNS
TOWER
CONFIGURATION
PLATFORM
FARM
UPS
DATABASE
CONCEPT
MANAGEMENT

LAYERS-FU: CAPABILITY NOT CATEGORY



- Hunting & Collaborating
- Integration & Automation
- Hardening & Prevention
- Retrospection
- Patterns of Attack Detection
- Indicator-based Detection
- Remediation
- Triage
- Visibility

LAYERS-FU: EFFECTIVE USE OF TIME




Increasing
Supply

YOU CAN'T STOP WHAT YOU CAN'T SEE

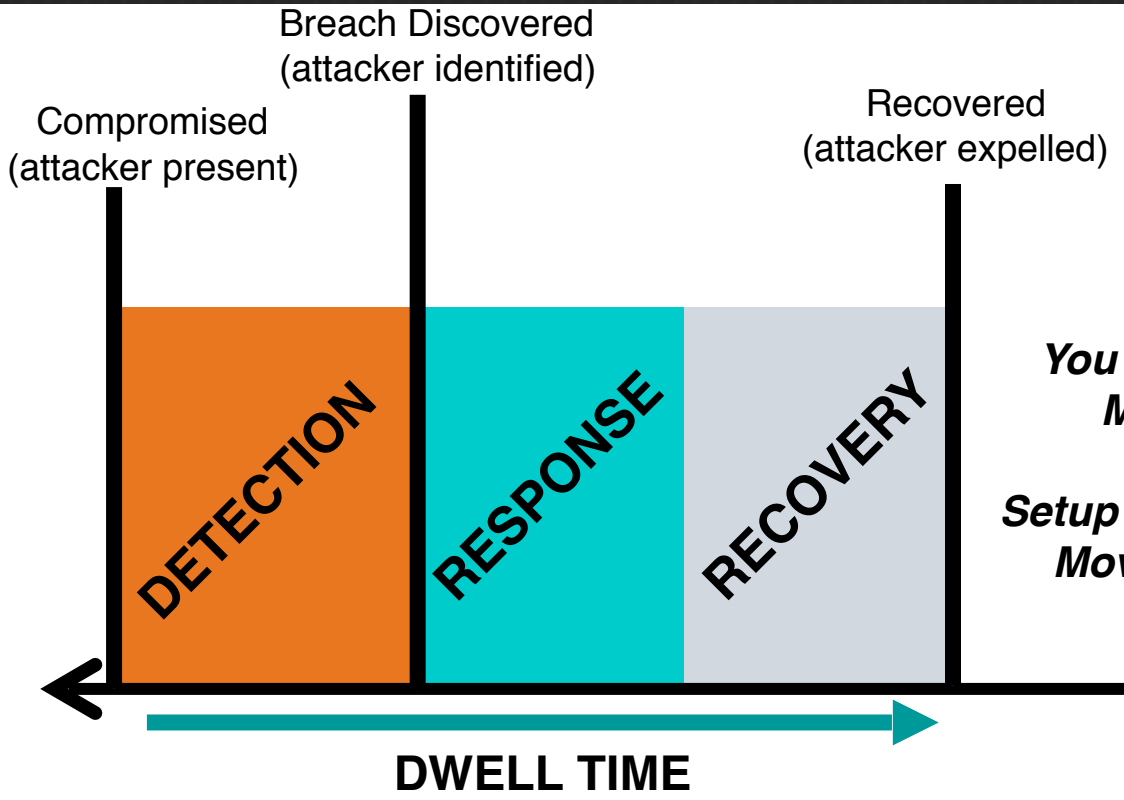
BEING REACTIVE IS NOT EFFECTIVE

Waiting for fires to put out!

HARVESTING ALERTS (FARMING)

DEMAND ON RESPONSE TIME (SUPPLY)?

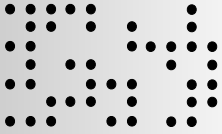
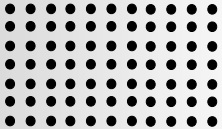
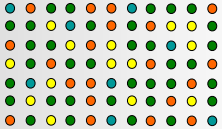
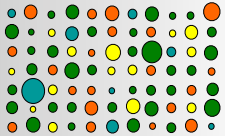
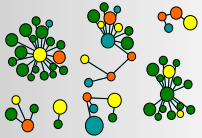
PRIORITIZE COLLECTION (VISIBILITY)



You know what questions you'll have…
Make sure you can answer them!

Setup the video camera before the robbery.
Move Fast, Don't Wait on Technology!

VISIBILITY: RELATIONSHIPS MATTER

Scanning	
Continuous Recording	
Continuous Recording + Intelligence	
Continuous Recording + Intelligence + Prevalence	
Continuous Recording + Intelligence + Prevalence + Relationships	


OUTSOURCING
CUSTOMER
COMMUNICATION
SERVICES
FUNCTION
PAYMENT
SATISFACTION
FINANCE
QUALITY OF SERVICE
COST
FUNCTION
STRATEGY
STRATEGY
ASSESSMENT
PROCESS
TRANSFERRING
SKILLS
STRATEGY
PROCESS
SERVICES
SKILLS
CONTEXT
PROCESS
COST
STRATEGY
SATISFACTION
CUSTOMER
SOFTWARE
CONTRACT
BUSINESS
RELATIONSHIP
SERVICES
EXPERTISE
FEEDBACK
SKILLS

FEEDBACK LOOPS

*Time is the dominant parameter. The pilot who goes through the **OODA** cycle in the shortest time prevails because his opponent is caught responding to situations that have already changed.*

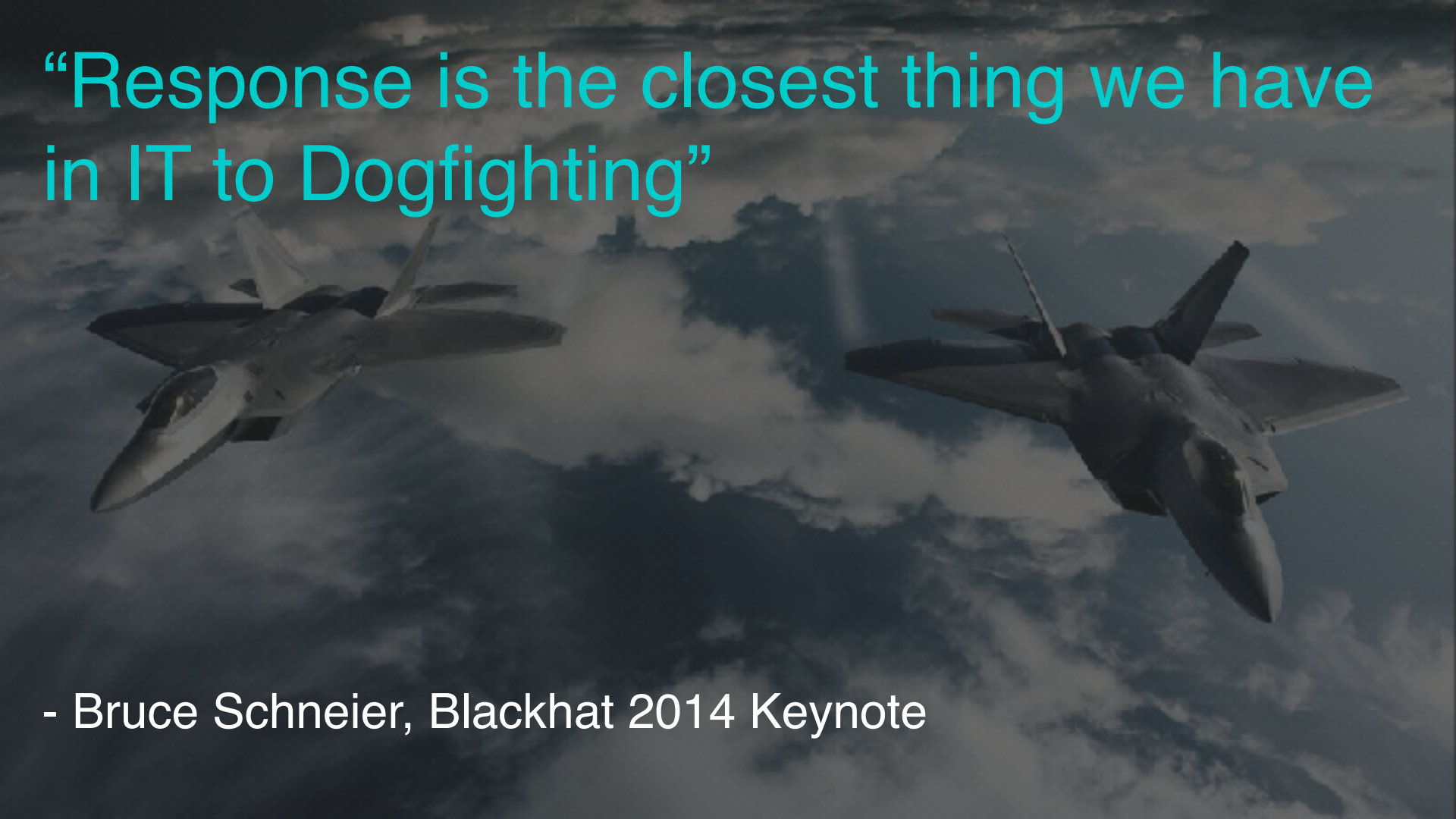
Col John Boyd
1966

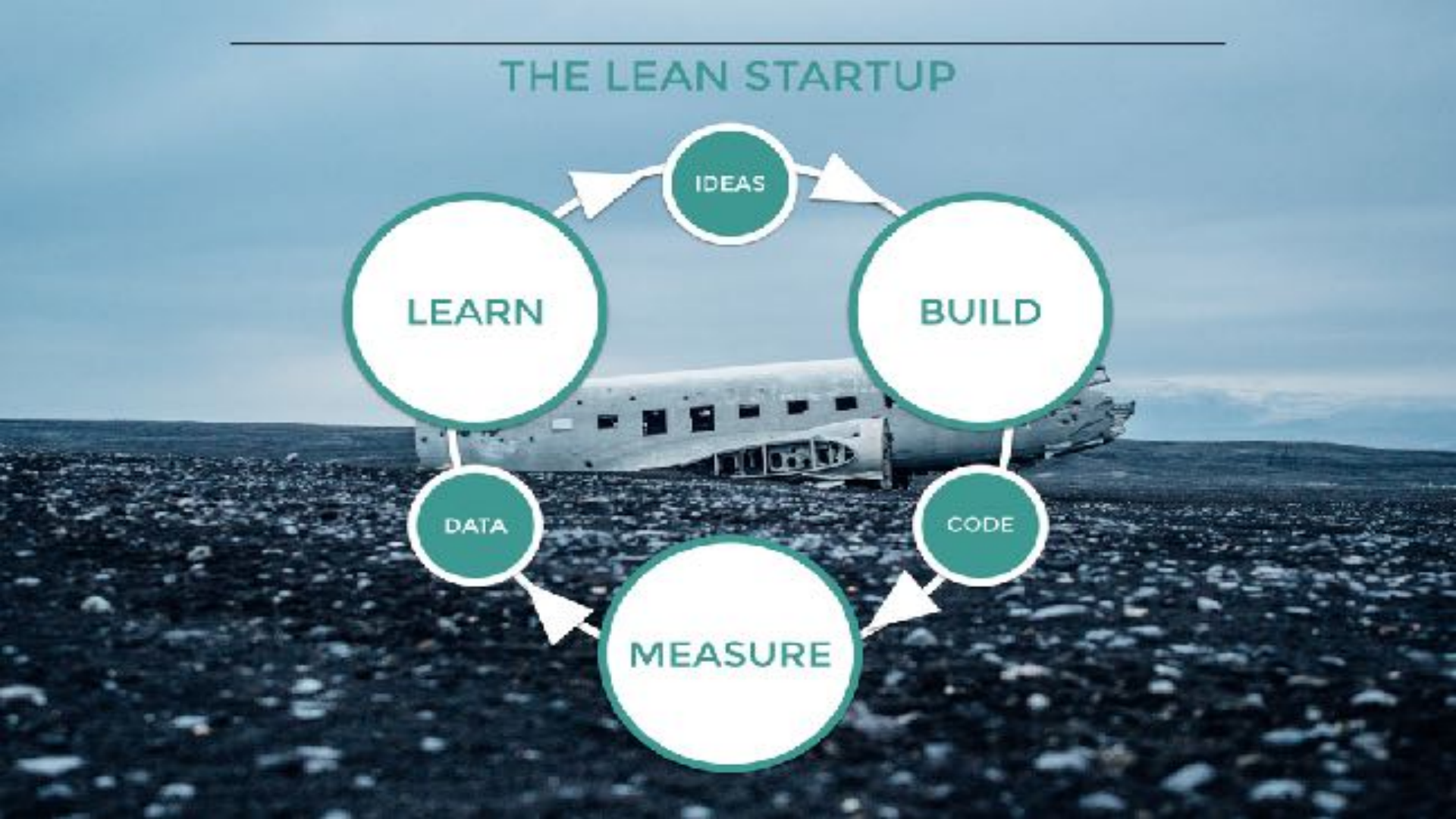
OBSERVE
ORIENT
DECIDE
ACT

SPEED IS ESSENTIAL

"A **good decision today** is **better** than a **great decision 48-hours** from now."

- US Military


“Response is the closest thing we have in IT to Dogfighting”
- Bruce Schneier, Blackhat 2014 Keynote


THE LEAN STARTUP
IDEAS
LEARN
BUILD
DATA
CODE
MEASURE

TEAM OF MAN-MACHINES

Generating Demand

EVOLVING THREAT LANDSCAPE

Cybercriminals

- Broad-based and targeted
- Financially motivated
- Getting more sophisticated

Hactivists

- Targeted and destructive
- Unpredictable motivations
- Generally less sophisticated

Nation-States

- Targeted and multi-stage
- Motivated by data collection
- Highly sophisticated with endless resources

Insiders

- Targeted and destructive
- Unpredictable motivations
- Sophistication varies

Threats Live off the Land (and Blend In)

Today we published our report on the untold story of the Target attack. The full version is available here.

announced that it had been breached by attackers who had gotten away with 70M customers' Personal Identifiable Information (PII). A few days later, Target admitted that 40M credit cards were stolen. The financial damages to Target currently stand at $148M, and according to analyst forecasts are estimated to reach $1B.

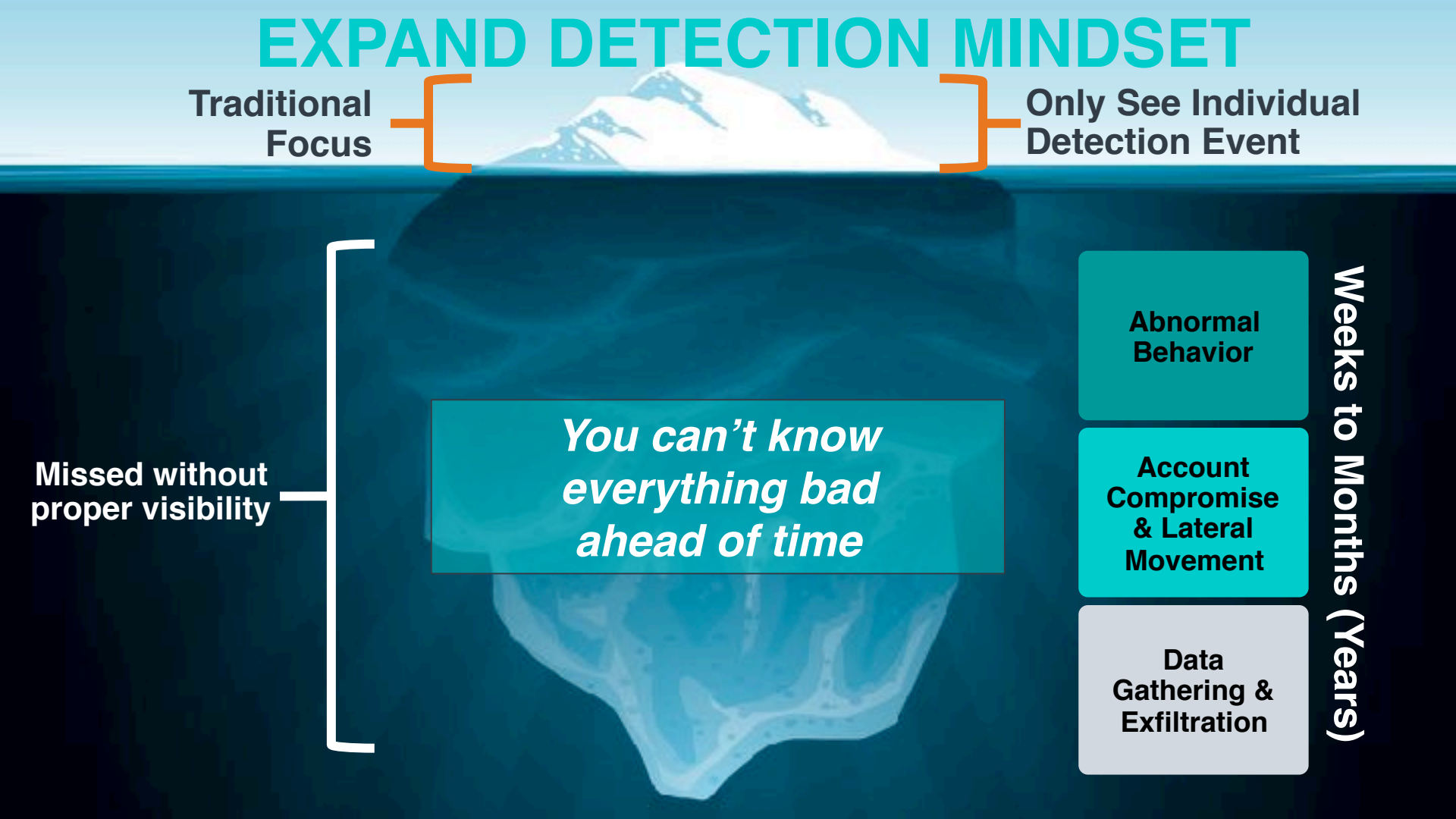
This report builds out the entire Target attack story and sheds light on the previously unanswered questions:

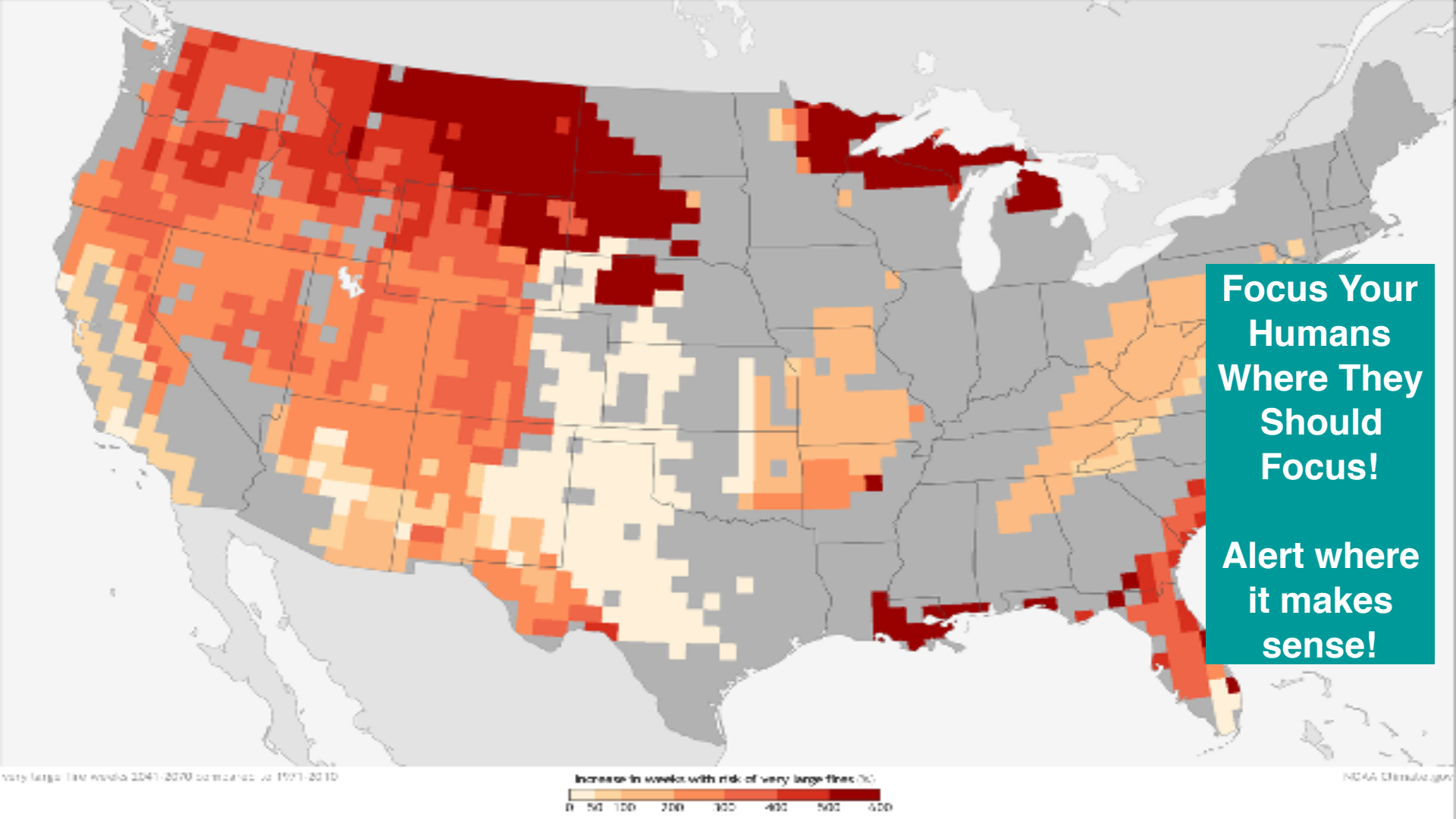
- How were the Target attackers able to leap from the machine of a sub-contractor to the heart of the payment systems?
- How did the attacker get a hold on some 70M "Personal Identifiable Information" (PII)?

The report reveals the attackers' Tactics, Techniques and Procedures (TTPs) and

- Attackers mostly used general IT tools, protocols and procedures. Seldom did they use hacker-specific tools and malware
- Active Directory related activity was paramount to the attackers' success
- Attackers used "Pass-the-Hash" techniques to propagate through Target's network
- Attackers had gained access to 70M PIIs by exploiting a SQL server database

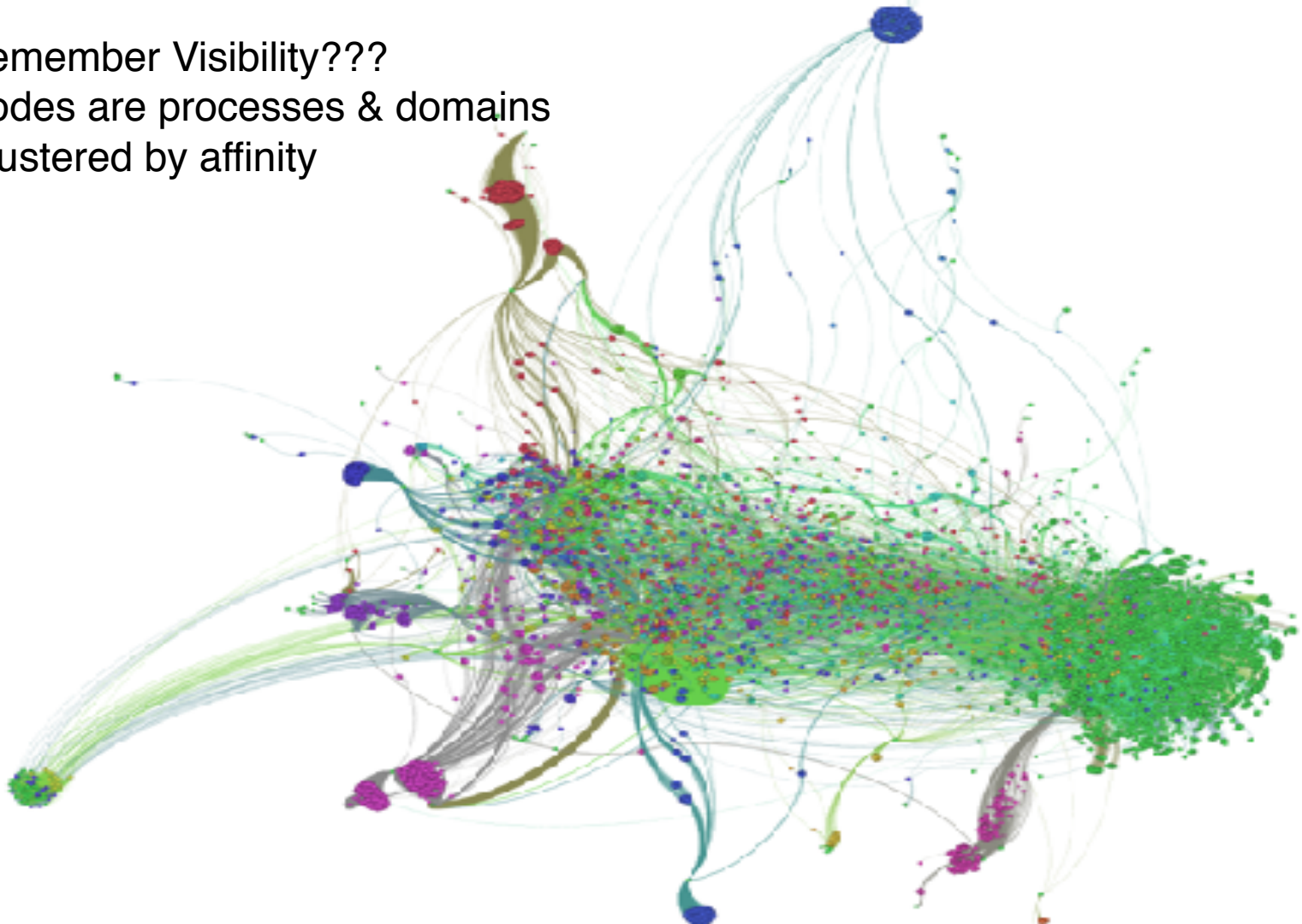
EXPAND DETECTION MINDSET




Focus Your Humans Where They Should Focus!
Alert where it makes sense!
Increase in weeks with risk of very large fires (%)
0 50 100 200 300 400 500 600

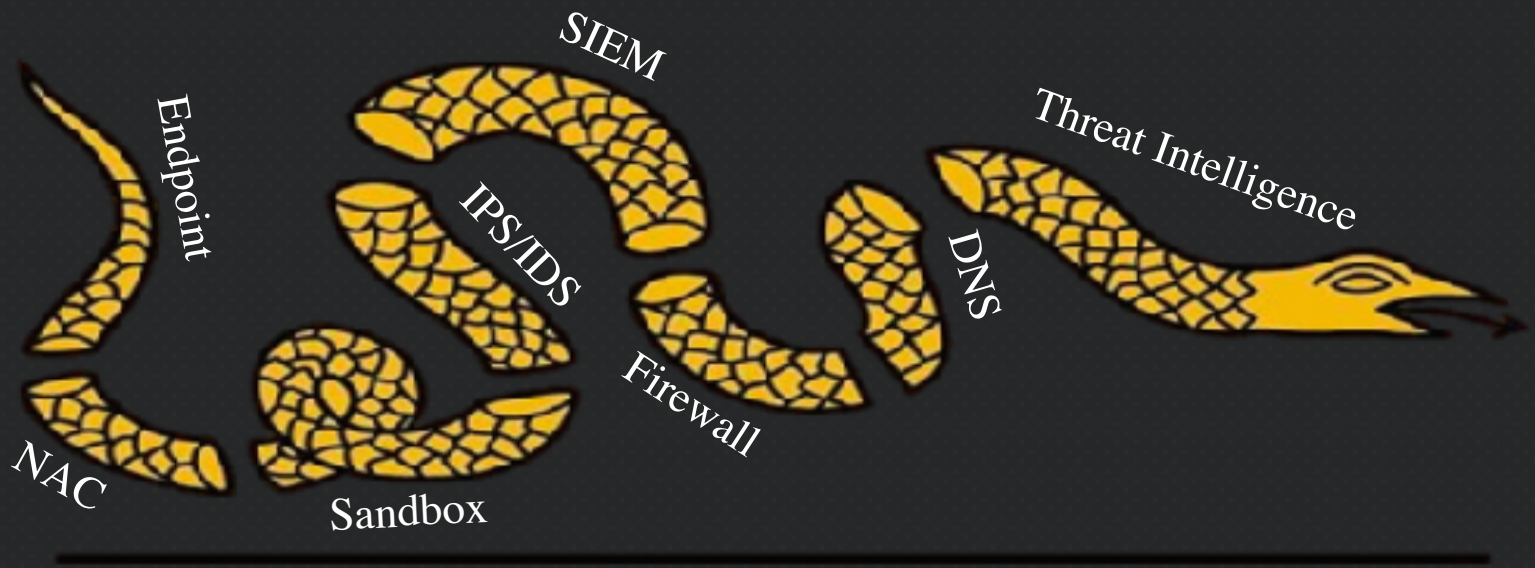

Greenland
Canada
United States
Mexico
Brazil
Argentina
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Finland
Sweden
Norway
United Kingdom
Poland
Germany
Ukraine
France
Spain
Kazakhstan
Mongolia
Russia
China
India
Saudi Arabia
Iraq
Algeria
Libya
Egypt
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Kenya
Angola
Namibia
Botswana
Madagascar
South Africa
Australia

Remember Visibility???
Nodes are processes & domains
Clustered by affinity



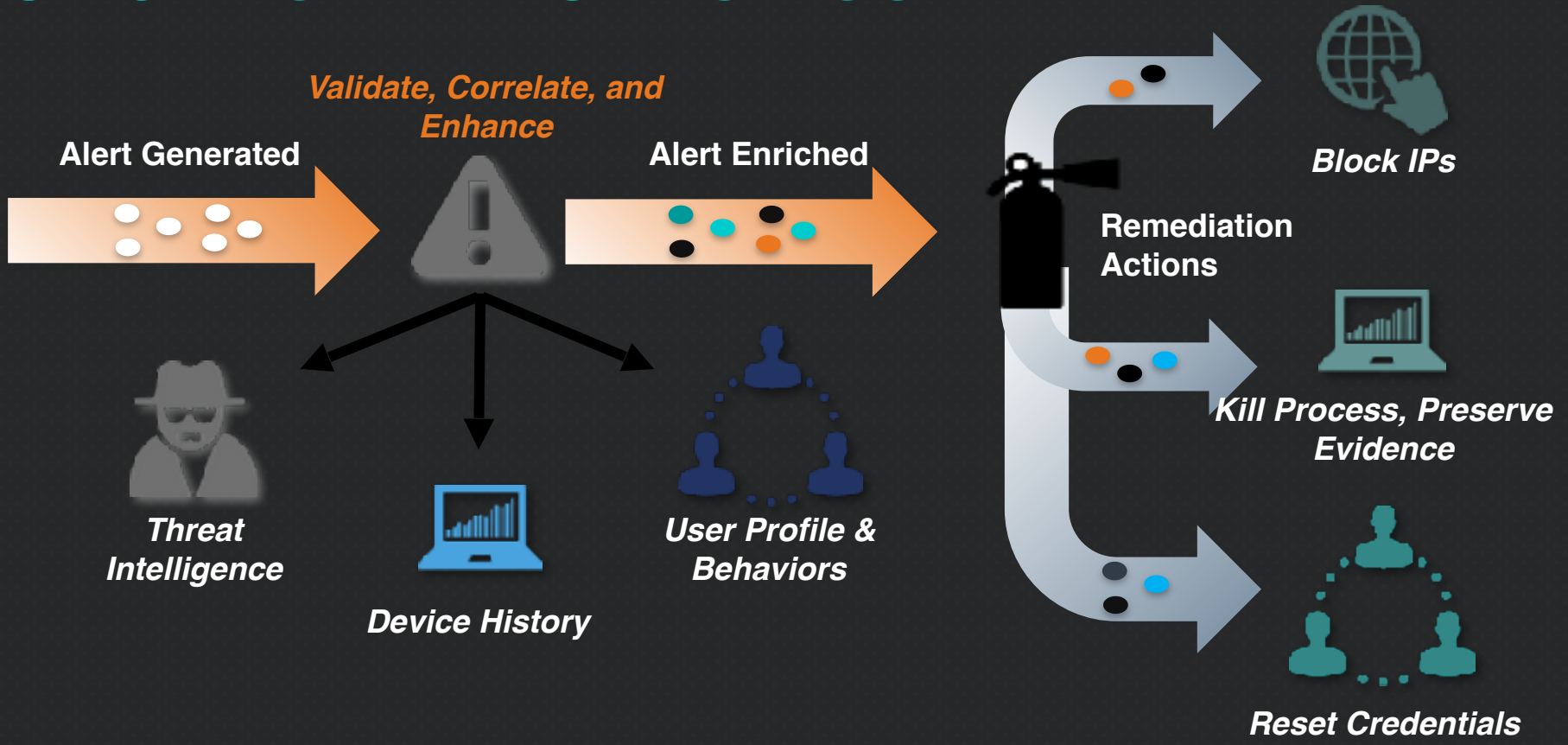

Creating
Leverage

Modern Security Stacks Are Blended



AUTOMATE, or DIE

ORCHESTRATION IS ESSENTIAL



AUTOMATION IS ESSENTIAL

“Today’s attackers have the upper hand due to the problematic economics of computer security. Attackers have the concrete and inexpensive task of finding a single flaw to break a system. Defenders on the other hand are required to anticipate and deny any possible flaw – a goal both difficult to measure and expensive to achieve.

Only automation can upend these economics.”

– **D**efense **A**dvanced **R**esearch **P**rojects **A**gency

https://nakedsecurity.sophos.com/2015/03/31/darpas-plan-to-make-software-security-the-domain-of-machines/

AUTOMATION ISN'T A SILVER BULLET

"The first rule of any technology used in a business is that **automation** applied to an **efficient** operation will **magnify** the **efficiency**. "

"The second is that **automation** applied to an **inefficient** operation will **magnify** the **inefficiency**."

- Bill Gates

TECH COMPANY – USE CASE

- **Pre-Orchestration**
  - 2 security engineers
  - **20-30 alerts a day**
  - **Manually processed 4-6 alerts day (<10%)**
  - Data aggregation to handle alert ~2 hours
  - (1 threat feed)
  - Minimal endpoint/user visibility (mostly threat)
  - No scoring information
  - **Time to resolution 5-10 days**
- **Post-Orchestration**
  - 2 security engineers
  - **50-200 alerts day**
  - **Automatically process 100% of alerts per day**
  - Data aggregation to handle alerts < 10 mins
  - (5 threat feeds)
  - Detailed endpoint/user visibility
  - (endpoint, user, asset posture)
  - Detailed scoring around threat, user, endpoint
  - **Time to resolution is <1hr**
- **Key points:**
  - **Orchestration allowed us to add additional pieces to the**
  - More alerts doesn't slow down resolution because automated
  - hindrance.
  - **Today it is easier to install new security technology than hire people to run it, therefore, orchestration alleviates lack of available security talent.**
  - Visibility in overlap of alerts, for example, network/endpoint alerts triggering at same relative time.
  - Centralized orchestration provides centralized visibility
  - Swapped out vendors with no APIs to 100% API based stacked to increase speed and maintainability.

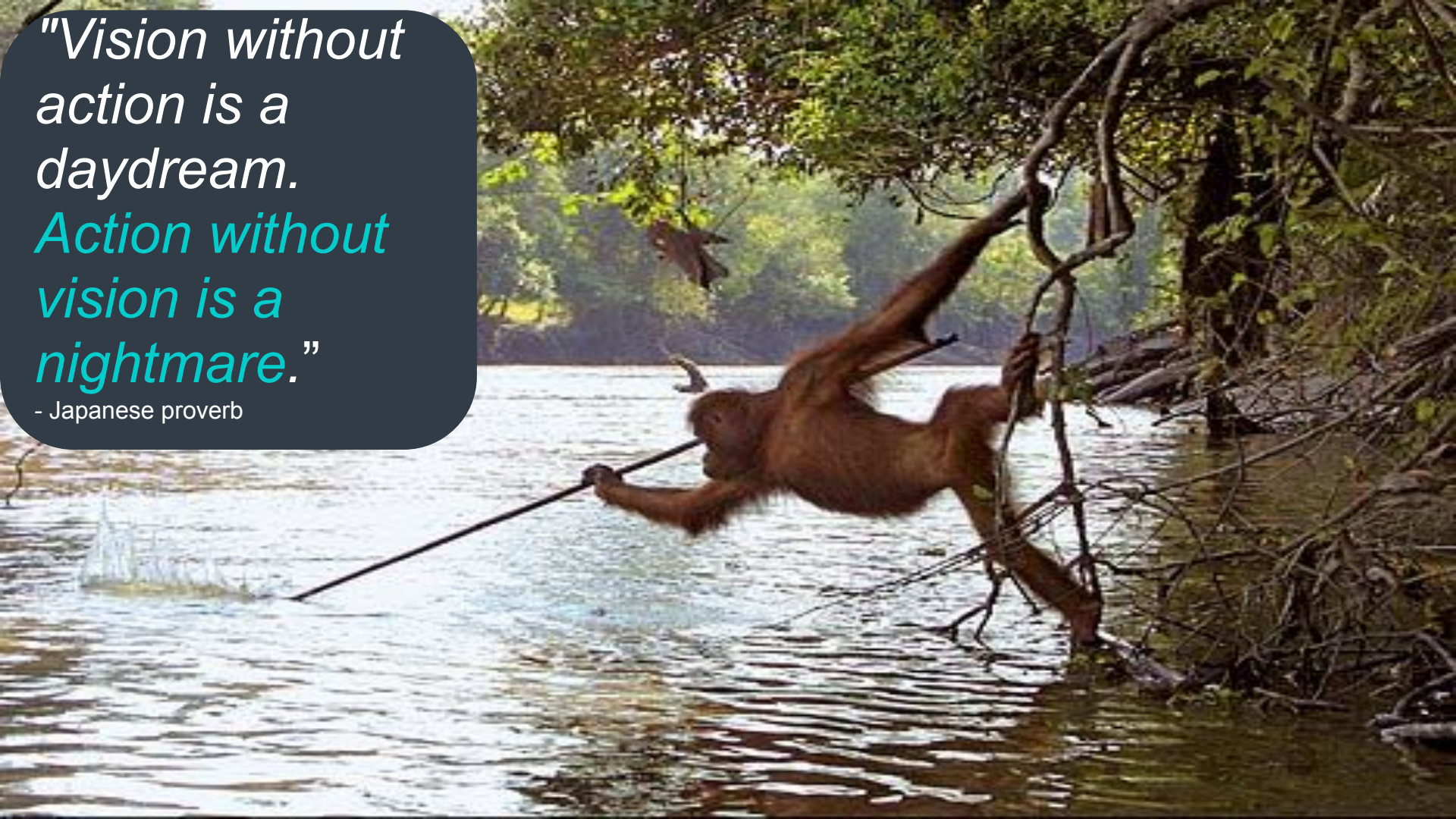
TECH COMPANY – SUMMARY

• Pre-Orchestration – 2 Sec Engineers • 20 alerts a day • Manually processed 4-6 alerts (20%) • Data aggregation ~2 hours • Time to resolution 5-10 days	• Post-Orchestration – 2 Sec Engineers • 200 alerts day • Automatically process 100% of alerts • Data aggregation ~10 mins • Time to resolution is <1hr

- **Orchestration** allowed us to **add** additional **pieces** to the stack to **cover more gaps without** an **increase** in **headcount**

- **Today** it is **easier** to **install new security technology** than **hire people** to run it, therefore, **orchestration alleviates lack of available security talent**.


HUNTING


"Vision without action is a daydream. Action without vision is a nightmare."
- Japanese proverb

HUNTING TIPS

- **ALLOW FOR CREATIVITY. ALLOW HUNTERS TO ‘EXPLORE’**
- LOOK FOR RISK. LOOK FOR THREATS.
- EXCHANGE INFORMATION QUICKLY
- LOOK ACROSS THE STACK – CONTEXT
- DON’T WAIT FOR MACHINES
- MAKE SURE THERE ARE LESSONS LEARNED FROM EACH HUNT

HUNTING OUTCOMES

- **NOT ALWAYS MALWARE OR APT OR MALICIOUS ACTIVITY.**
- WHERE TO HUNT?
- WHAT TO HUNT?
- WHERE ARE MY GAPS?
- WHERE ARE MY STRENGTHS?
- WHERE DO I NEED MORE CARE AND FEEDING?

COLLABORATE, SHARE, LEARN, EVOLVE!


WRAPPING
UP

Breach Discovery's *very nature requires the human element*

In IT, we hire staff to support technology

In security operations, we buy technology to support staff

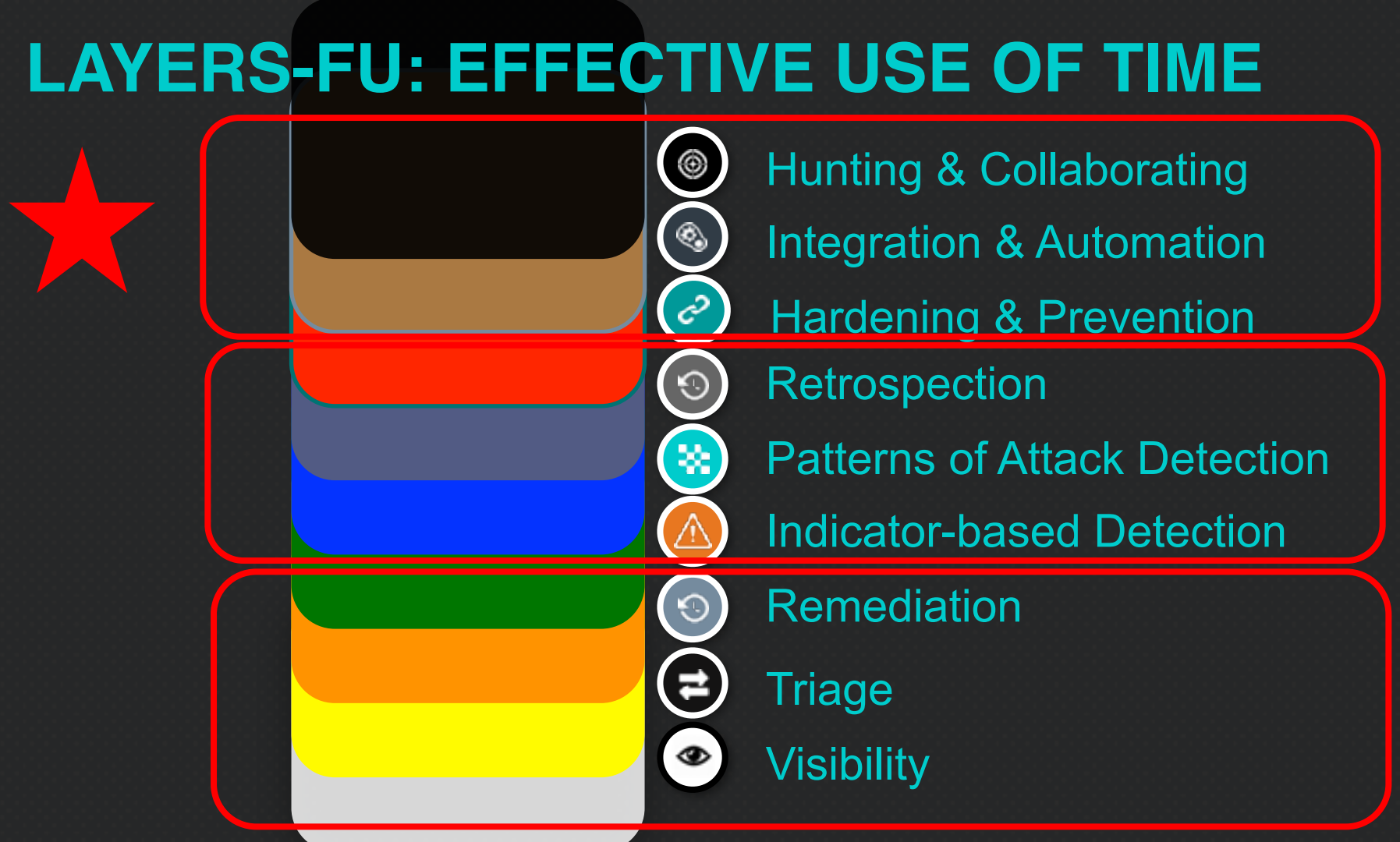
Enable humans to make ***quicker*** *decisions*

COMPROMISE IS INEVITABLE

Attacker only has to be successful **once**, but **defender** has to stop **100% of attacks**

Once the attacker is in **your environment**, ***they should have to be 100% perfect.***

LAYERS-FU: EFFECTIVE USE OF TIME



“It is about **making** the **wisest** possible **investment** of **your time** and energy in order to **operate** at our **highest** point of **contribution** by **doing** only what is **essential**.”

– *Greg McKeown, Author of Essentialism*

ARE YOU AIMING FOR THIS?

OR THIS?

THE REAL WORLD??

Ok, But You Need Actionable Tips…

- Back to the basics - work with IT
- Pick a tool, leverage the hell out of it
- Reduce Scope — small wins are great!
- Focus on ROI of your time


How are you spending your time?
What's essential?

THANK YOU

https://twitter.com/**chicagoben**
https://www.linkedin.com/in/**benjaminjohnson80**
ben@1011vc.com