Lean Hunting

SANS THIR SUMMIT 2018 | New Orleans, LA

Ben Johnson, Co-Founder & CTO

ben@obsidiansecurity.com

OBSIDIAN

OBSIDIAN

Abstract

Lean Hunting

(Threat) Hunting has been around long enough that most agree it should be part of all comprehensive information security programs. In any cat and mouse game, existing traps will never catch all mice. We need to apply creativity, analytical thinking, and keep humans in the loop. The challenge, of course, is that human hours are scarce and expensive. Most organizations cannot afford to staff hunt teams 24/7 (or at all), so what's the best way to deploy human attention to identify emerging threats? We'll explore how to adopt aspects of entrepreneurship and align organizations to achieve positive outcomes by building lean (threat) hunting capabilities.

@chicagoben I @obsidiansec

Agenda

Introduction

State of Cyber

Entrepreneurship

Applied Lean Hunting

Wrap-Up

Background Check

Ben Johnson
Co-Founder and CTO, Obsidian Security

Co-founder and former CTO of Carbon Black, built the first EDR product. Previously, NSA CNO and AI Lab.

2000 2010 2017

Career NSA → Carbon Black. → OBSIDIAN

Board Seats SENRIO, CAPSULE8, EVOLVE Security Academy, ACALVIO

Entrepreneurship Professor THE UNIVERSITY OF CHICAGO

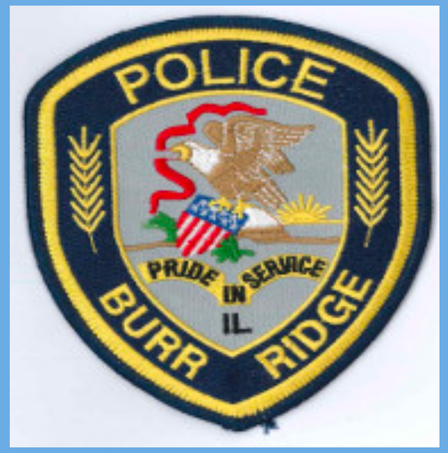
Today's Goal?

TO SPARK CONTEMPLATION

(and hopefully give you a tip or two.)

OBSIDIAN

Physical-World IR



Recent headlines

Forbes

WOMEN@FORBES SEP 25, 2017 @ 05:21 PM

Deloitte Hack May Have Exposed Emails, Passwords Of Clients And Staff

threatpost CATEGORIES FEATURED PODCASTS VIDEOS

LEAKY WWE DATABASE EXPOSES PERSONAL DATA OF 3M WRESTLING FANS

DARKReading Join us live at INSECURITY | A Dark Reading Conference

7/12/2017 05:50 PM

Verizon Suffers Cloud Data Leak Exposing Data on Millions of Customers

cyberscoop

TRANSPORTATION HEALTHCARE TECHNOLOGY FINANCIAL WATCH LISTEN

GOVERNMENT

Booz Allen Hamilton leaves 60,000 unsecured DOD files on AWS server

The Hacker News™ Security in a serious way

Sweden Accidentally Leaks Personal Details of Nearly All Citizens

Monday, July 24, 2017 Swati Khandelwal

THE HILL

Dow Jones customer data exposed in cloud error

BY MORGAN CHALFANT - 07/17/17 11:23 AM EDT

ZDNet

OneLogin security chief reveals new details of data breach

Two breaches in as many years. Is the trust gone? Alvaro Hoyos, the company's chief information security officer, answered key questions.

SC MEDIA

SC US SC UK NEWS CYBERCRIME NETWORK SECURITY PRODUCT REVIEWS IN DEPTH EVENTS WHITEP

THE CYBERSECURITY SOURCE

October 12, 2017

Another AWS leak exposes 150,000 Patient Home Monitoring Corp. client records

GIZMODO

PRIVACY AND SECURITY

Viacom Leak May Have Exposed Hundreds of Digital Properties—Paramount Pictures, Comedy Central, MTV, and More

Dell Cameron 9/19/17 12:01pm • Filed to: DATA BREACHES

CNN tech

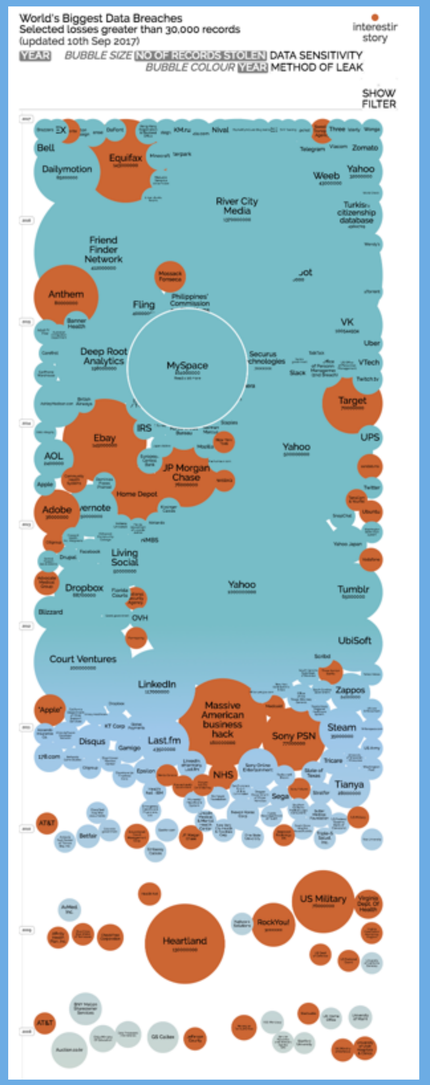
Cyber-Safe

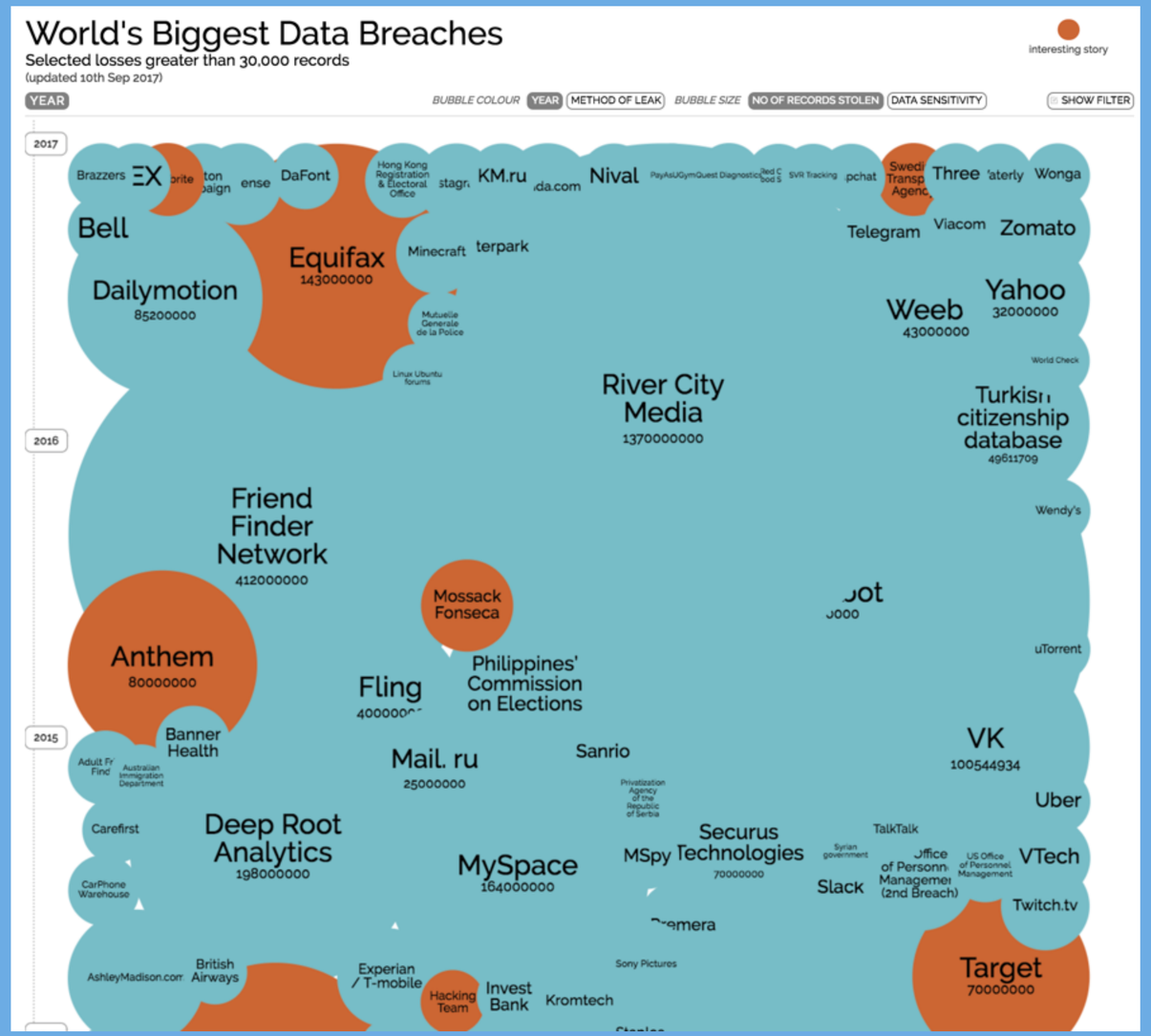
Data of almost 200 million voters leaked online by GOP analytics firm

by Selena Larson @selenalarson

June 19, 2017: 11:32 PM ET

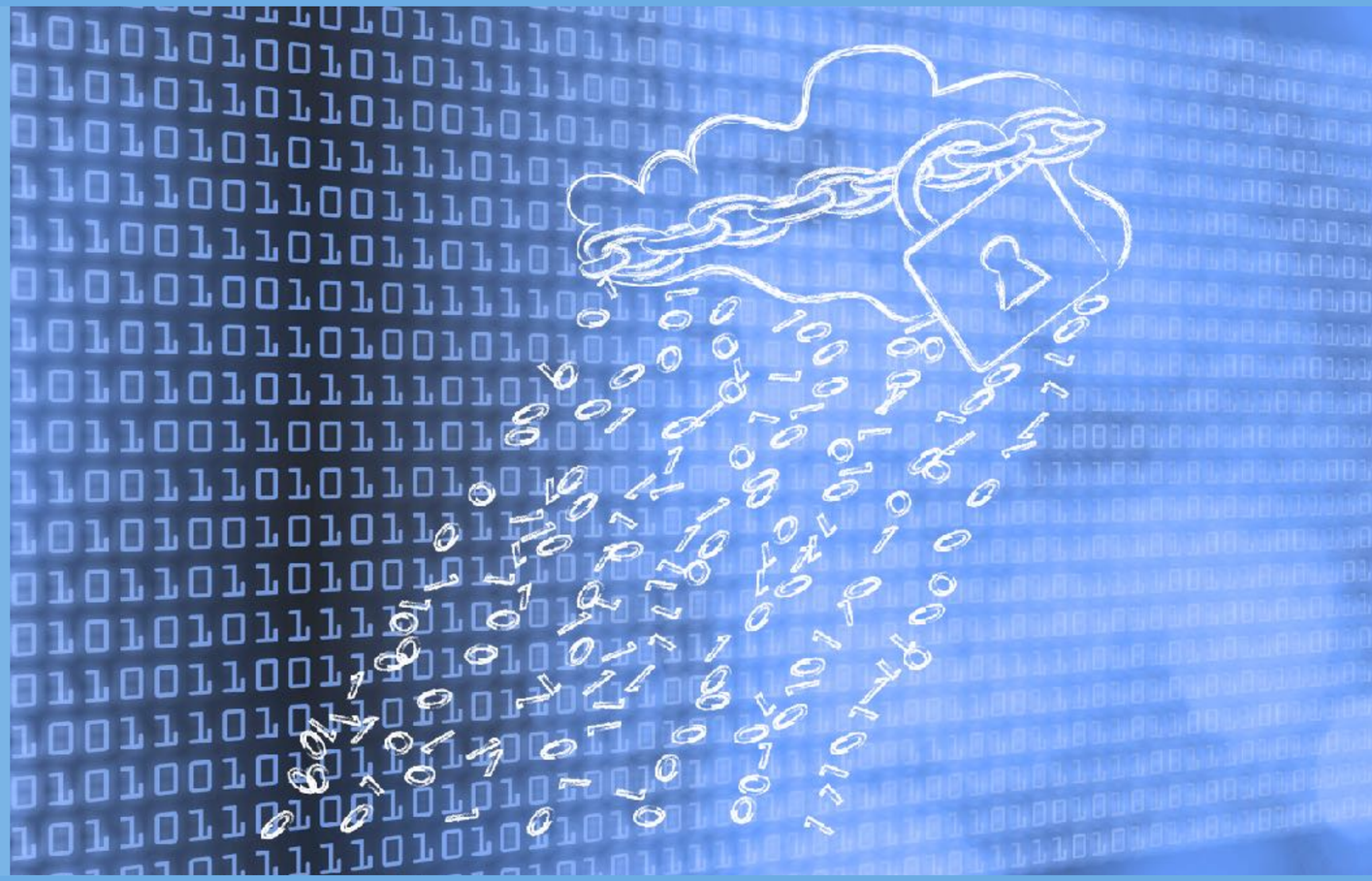
Data breaches





Even the Cloud is Leaky

Booz Allen
OneLogin
The RNC
Verizon
Accenture
Dow Jones
Viacom
Deloitte
Sweden
California



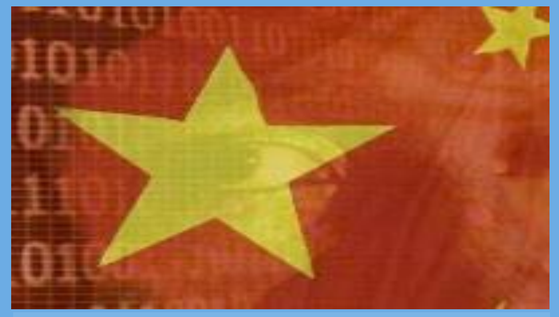
Variety of adversaries

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

Many challenges

Skills Gap +

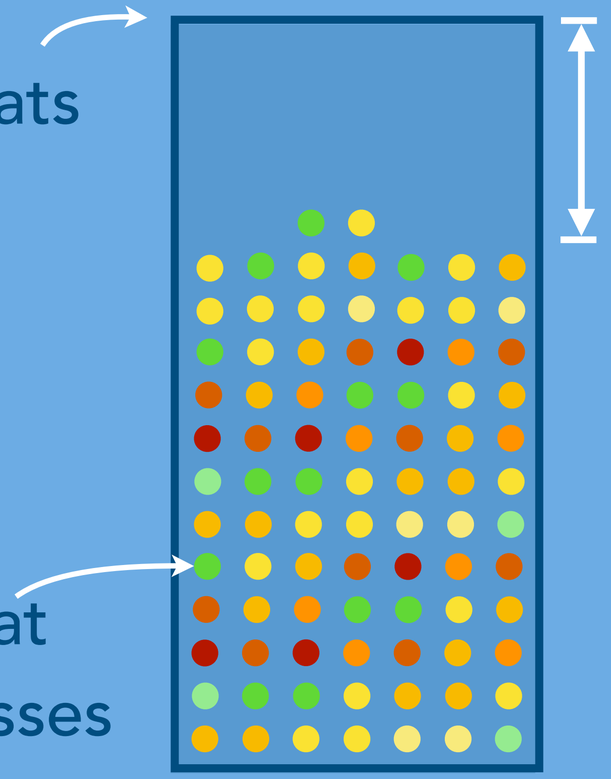
Deploy-and-Decay +

Attacker Successes +

Huge Data (more than big)

= LACK OF CYBER SELF-ESTEEM

Hunting: Filling the Automation Gap



Hunting: because there's always a gap between automated threat detection and the universe of threats.

Hunting: Ideal vs. reality

Ideal

Reality

Can hunting be formulaic?

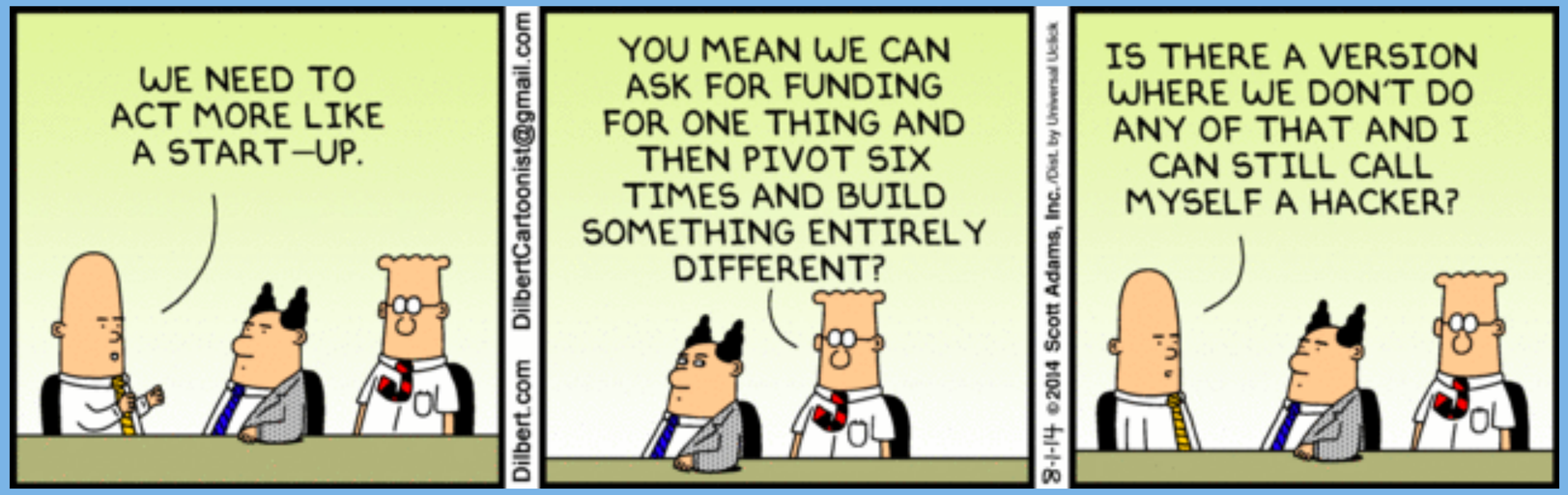
What's the formula for hunting?

$$X_{FTE} * Y_{tooling} + Z_{buy\text{-}in} \stackrel{?}{=} \text{Threat Hunting}$$


Entrepreneurship

Start-Up Formula?

What's the formula for start-ups?



$$Idea^{(quality)} + work^{(quantity)} + raise\ money\ ?= profit$$

Lean Manufacturing

- Developed by Toyota 70s/80s, perhaps 30s!
- Systematic, holistic identification of waste
- Improves the flow / smoothness of work
- Just-In-Time and Autonomation (smart automation)
- Identify features, process, inputs that create customer value, *everything else is waste*

Lean Manufacturing

Eight types of waste require monitoring:

1. **Overproduction** – Is supply way higher than demand?
2. **Waiting** – Lag time between production steps
3. **Inventory** (work in progress) – Are supply levels and work in progress inventories too high?
4. **Transportation** – Do you move materials efficiently?
5. **Over-processing** – Do you work on the product too many times?
6. **Motion** – Do people and things move between tasks efficiently?
7. **Defects** – How much time do you spend finding, fixing mistakes?
8. **Workforce** – Do you use workers efficiently?

Waste:
anything that doesn't add value to the end product

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

Lean Startup Methodology

"The Lean Startup method teaches you how to drive a startup - how to steer, when to turn, and when to persevere - and grow a business with maximum acceleration."
- Eric Ries

Lean methodology:

- Gets products and services in the hands of customers faster.
- Reduces uncertainty (and waste)!

Entrepreneurs are Everywhere

"The day before something is a breakthrough, it's a crazy idea."

- Peter Diamandis

Think Big.

Start Small.

Scale Fast.

Validated Learning

How quickly can you learn?

"Are you learning in gulps or sips?"
- Apollo Astronauts

It's all about product-market fit!

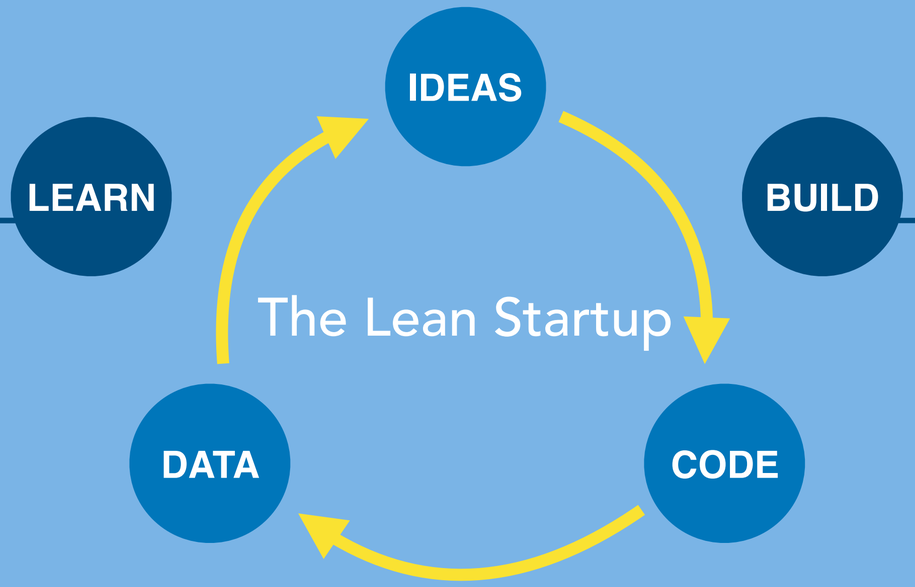
Create hypothesis.

Run Experiment.

Analyze Results.

Repeat.

Build. Measure. Learn



Learn Faster

- Unit Tests
- Customer interviews
- Customer development
- Five whys root cause analysis
- Customer advisory board
- Justifiable hypothesis
- Product owner accountability
- Custom archetypes
- Cross-functional team
- Smoke tests

Build Faster

- Unit tests
- Usability tests
- Continuous integration
- Incremental deployment
- Free & open-source components
- Cloud computing
- Cluster immune system
- Just-in-time scalability
- Refactoring
- Developer sandbox

Measure Faster

MEASURE

- Split tests
- Clear product owner
- Continuous development
- Usability Tests
- Real-time monitoring
- Customer Liaison
- Funnel analysis
- Cohort analysis
- Net promoter score
- Search engine marketing
- Real-time alerting
- Predictive monitoring

Wait ... OODA 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."

- Colonel John Boyd, 1966

Observe.

Orient.

Decide.

Act.

Minimum Viable Product.

Minimum viable product: The skinniest version of a product that still functions.

- sufficient functionality to attract initial users/customers
- promises enough future benefit to keep early adopters
- designed with a feedback loop to guide new features

What's the MVP you think is necessary?


Applied
Lean Hunting
OBSIDIAN
@chicagoben | @obsidiansec

Building

What is your pain point?

"If I had an hour to solve a problem I'd spend 55 minutes thinking about the problem and 5 minutes thinking about solutions."

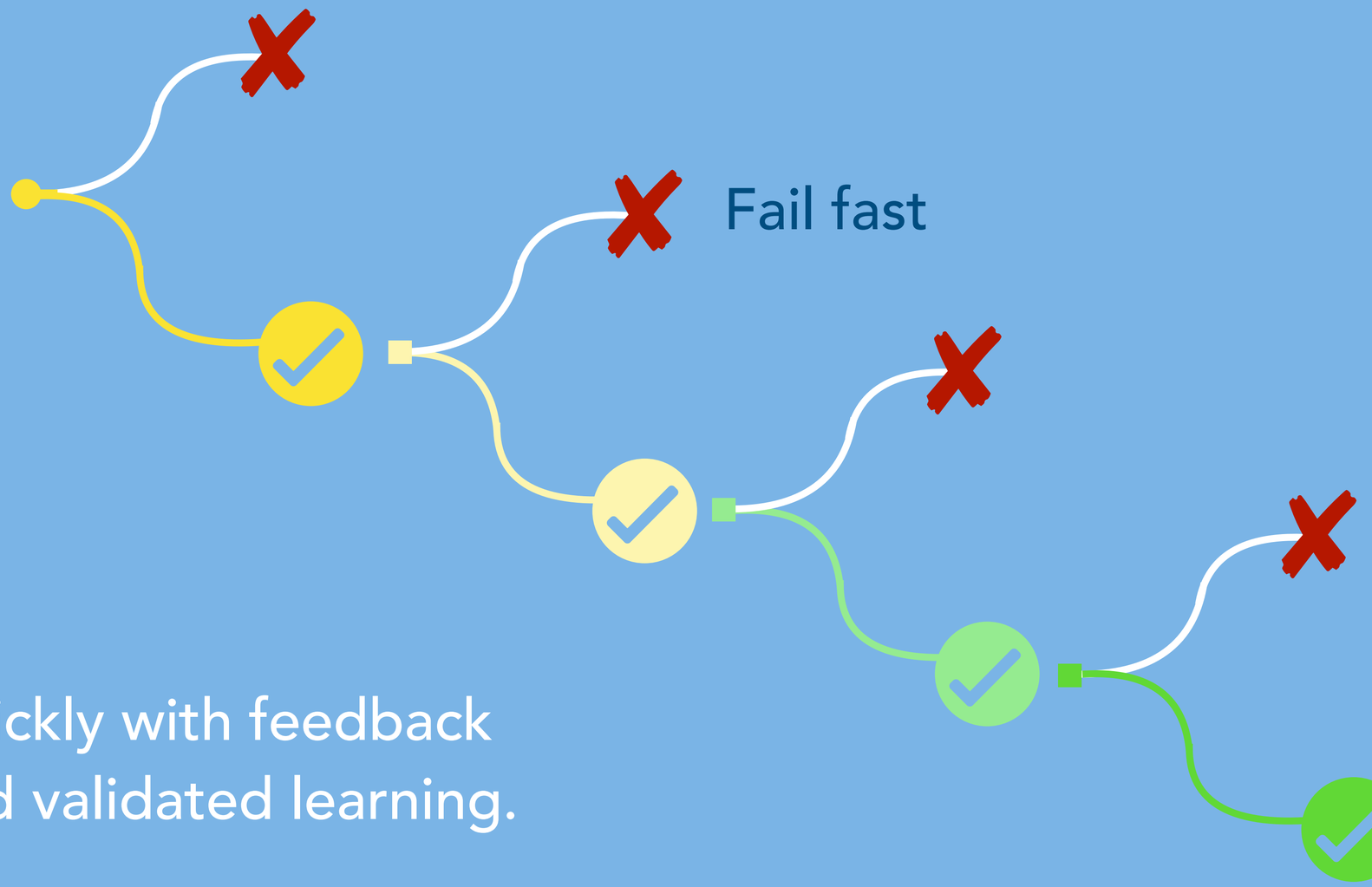
- Albert Einstein

Who is this for?

What is this for?

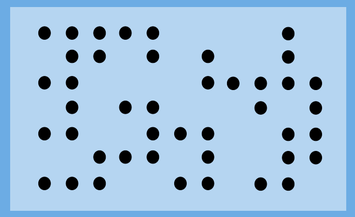
Painkillers vs Vitamins

Efficient Hunting (& Triage): Fail Fast

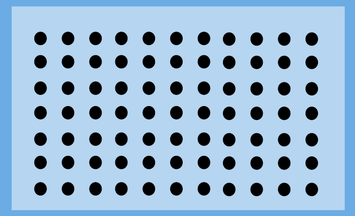


Move quickly with feedback loops and validated learning.

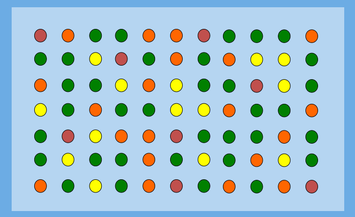
Building: Start with visibility



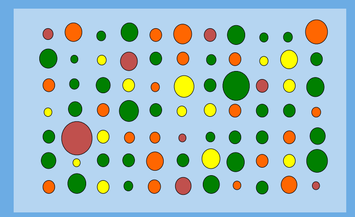
Scanning



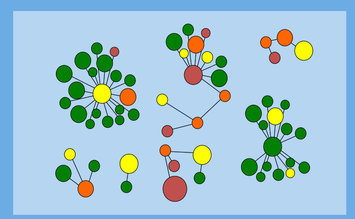
Continuous Recording



Continuous Recording + Intelligence



Continuous Recording + Intelligence + Prevalence

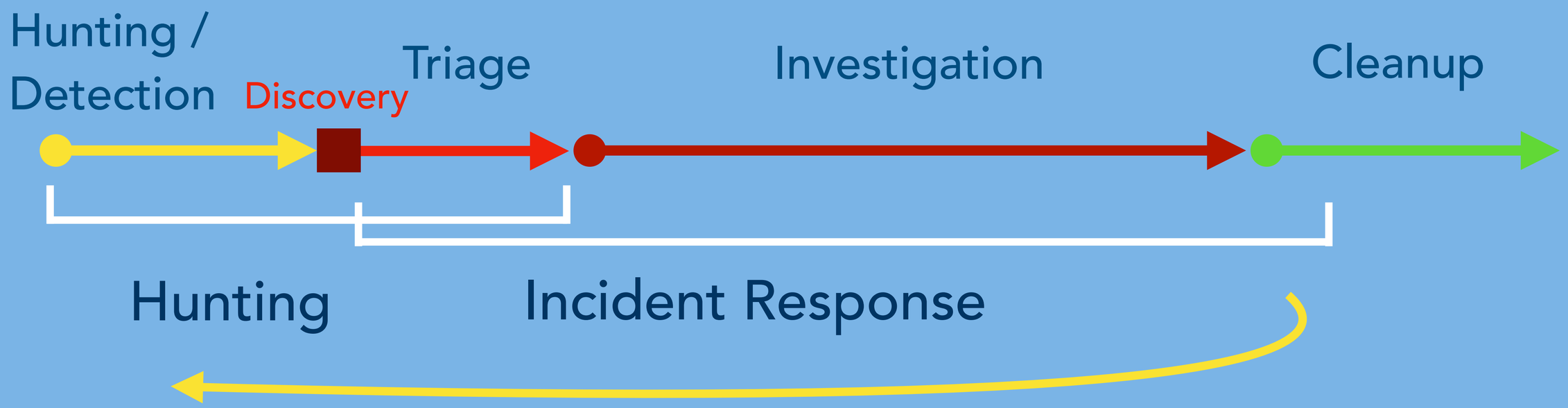


Continuous Recording + Intelligence + Prevalence + Relationships

Building: Open Source & APIs

elasticsearch

The Detection-Response Spectrum



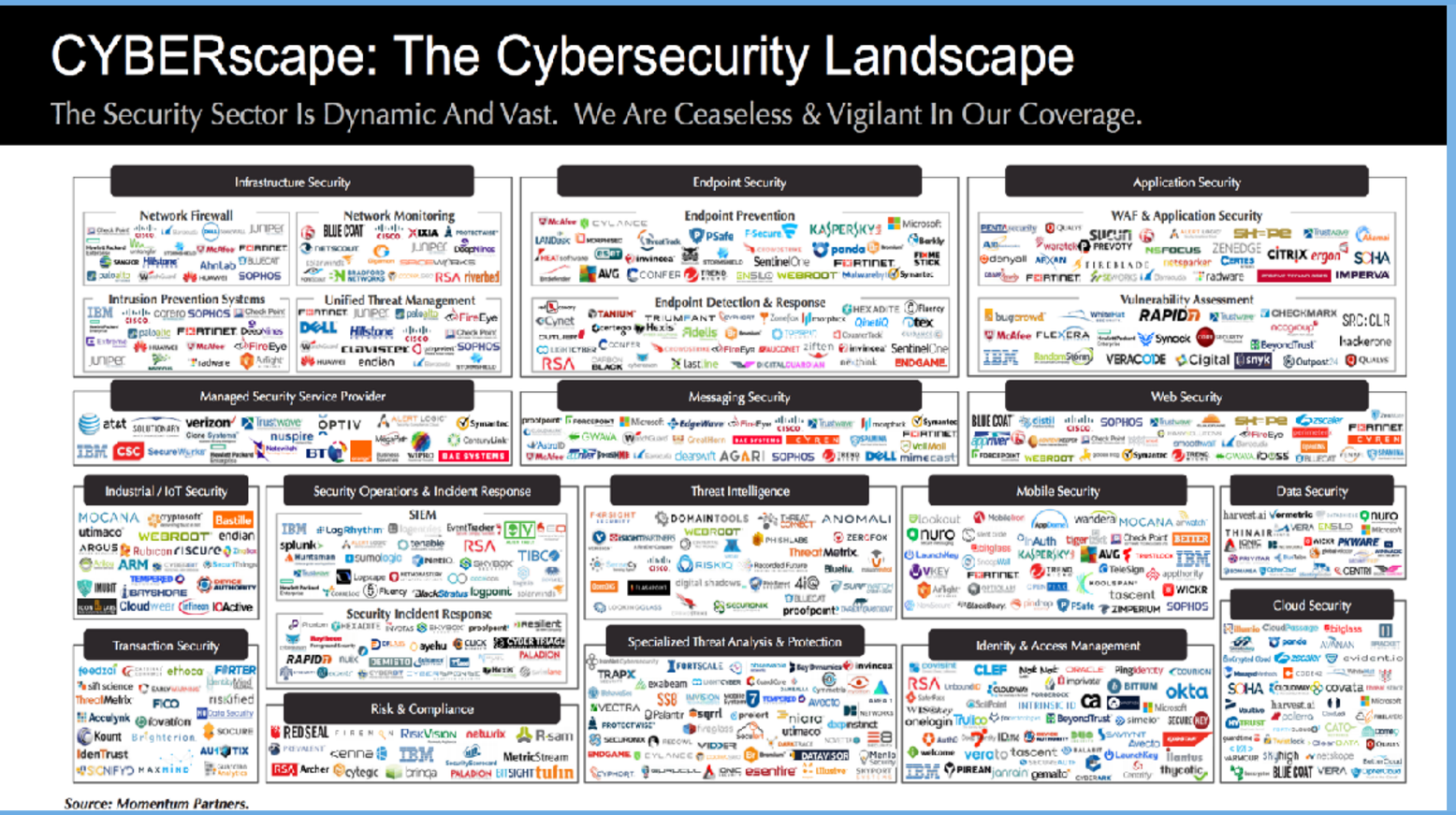
Selling

Can you sell your organization on new spending?

Can you sell your organization on freeing up time to hunt?

Can you sell the culture on spending time to help with hunting?

Competition



Source: Momentum Partners.

Can your competition (i.e. other tasks) be automated?

Can you make vendors better?


Wrap-Up (&Ranting)

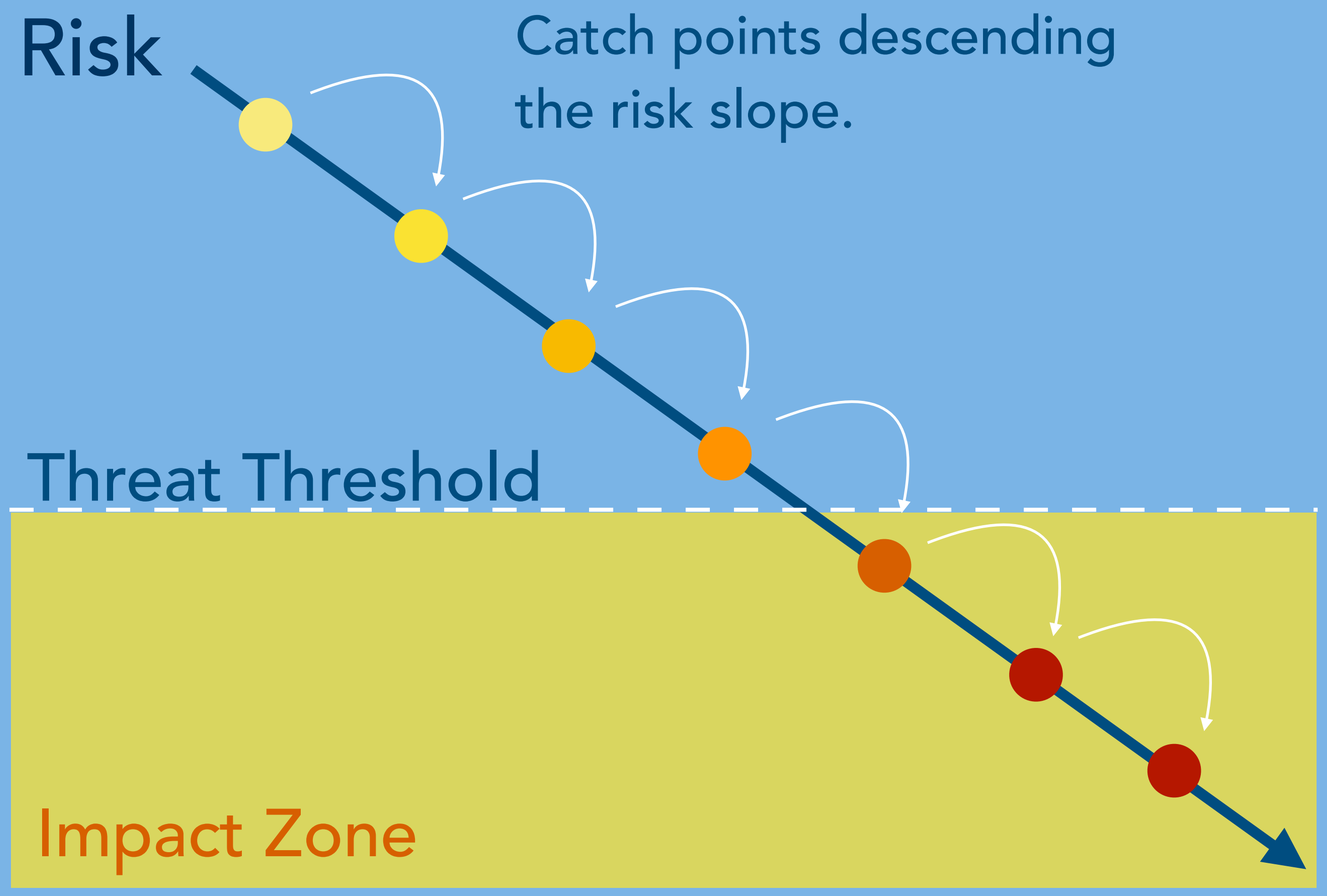
Is the Environment Healthy?

The absence of disease does not mean health.

Reduce Entropy, Reduce Risk

OBSIDIAN

Risk as a Slope



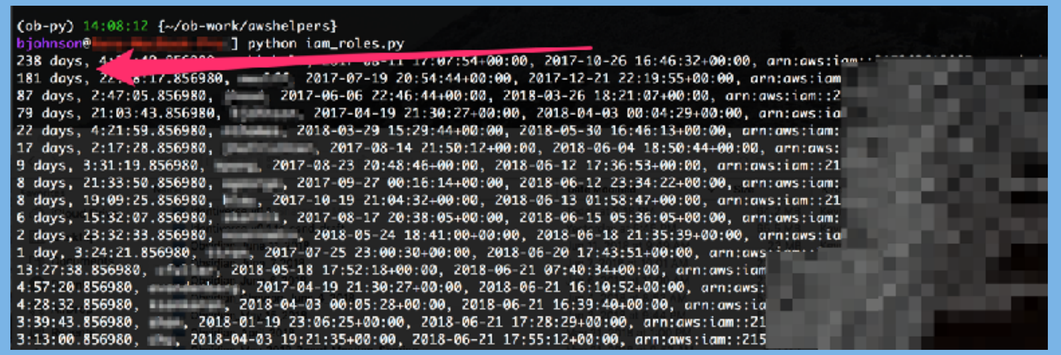
The steeper the risk slope, the faster the environment slides into compromise.

Reduce risk, reduce the slope!

Identity Creep

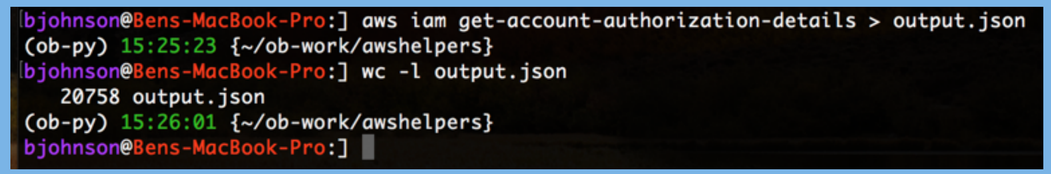
DORMANT ACCOUNTS

238 days
181 days
87 days
79 days
22 days
17 days
9 days
8 days

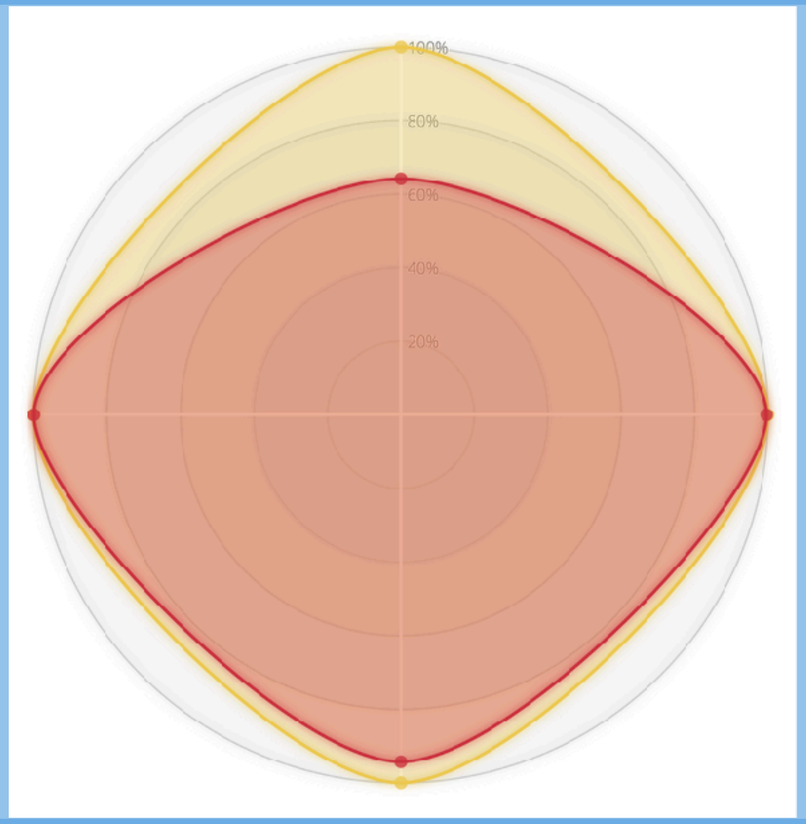


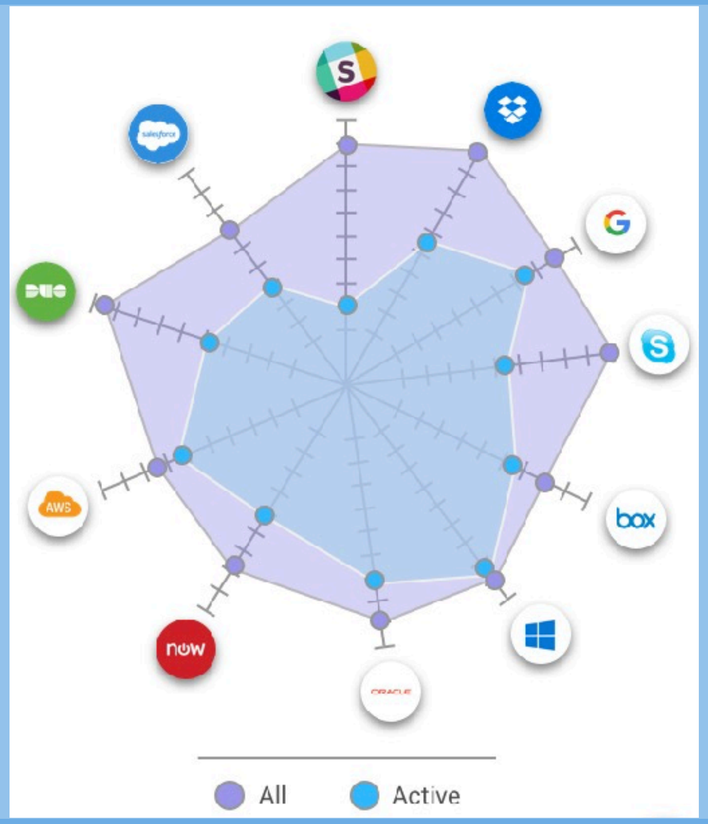
MISMATCHED PERMISSIONS

20758 lines



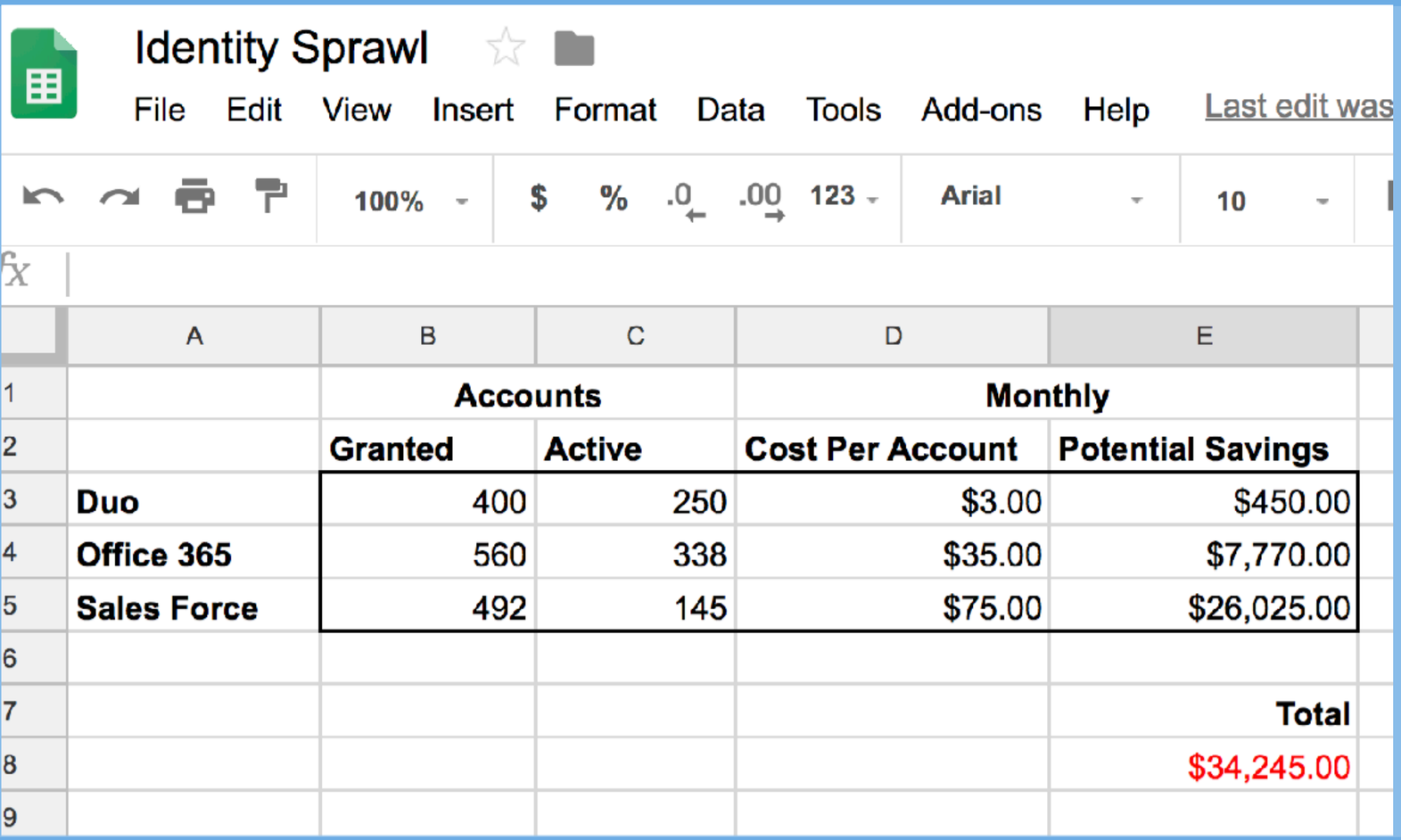
Right-Size Surface Area?





Visualize the surface area you *could* use against the surface area you *are* using. Lower the risk and also focus your hunts!

Dormant Accounts?



	A	B	C	D	E
1		Accounts		Monthly	
2		Granted	Active	Cost Per Account	Potential Savings
3	**Duo**	400	250	$3.00	$450.00
4	**Office 365**	560	338	$35.00	$7,770.00
5	**Sales Force**	492	145	$75.00	$26,025.00
6					
7					**Total**
8					$34,245.00
9					

Aside from risk, cost savings could be huge!

At left, a relatively small company (600 employees) could save over $300k / year by right-sizing 3 services!

Information Security and the Cloud

"IT is going from 0 to 100 in the cloud and leaving us in the dust"
- CISO, Financial Tech Company

"We're blind to all these new SaaS accounts"
- Director, Cyber Intelligence, Top Athletics Brand

"50% of our IR Engagements are Office 365."
- Principal IR, Rapid7

"We have 300 AWS accounts and no governance"
- Public Tech Company

"Hackers don't break in, they login." - CISO, Cisco

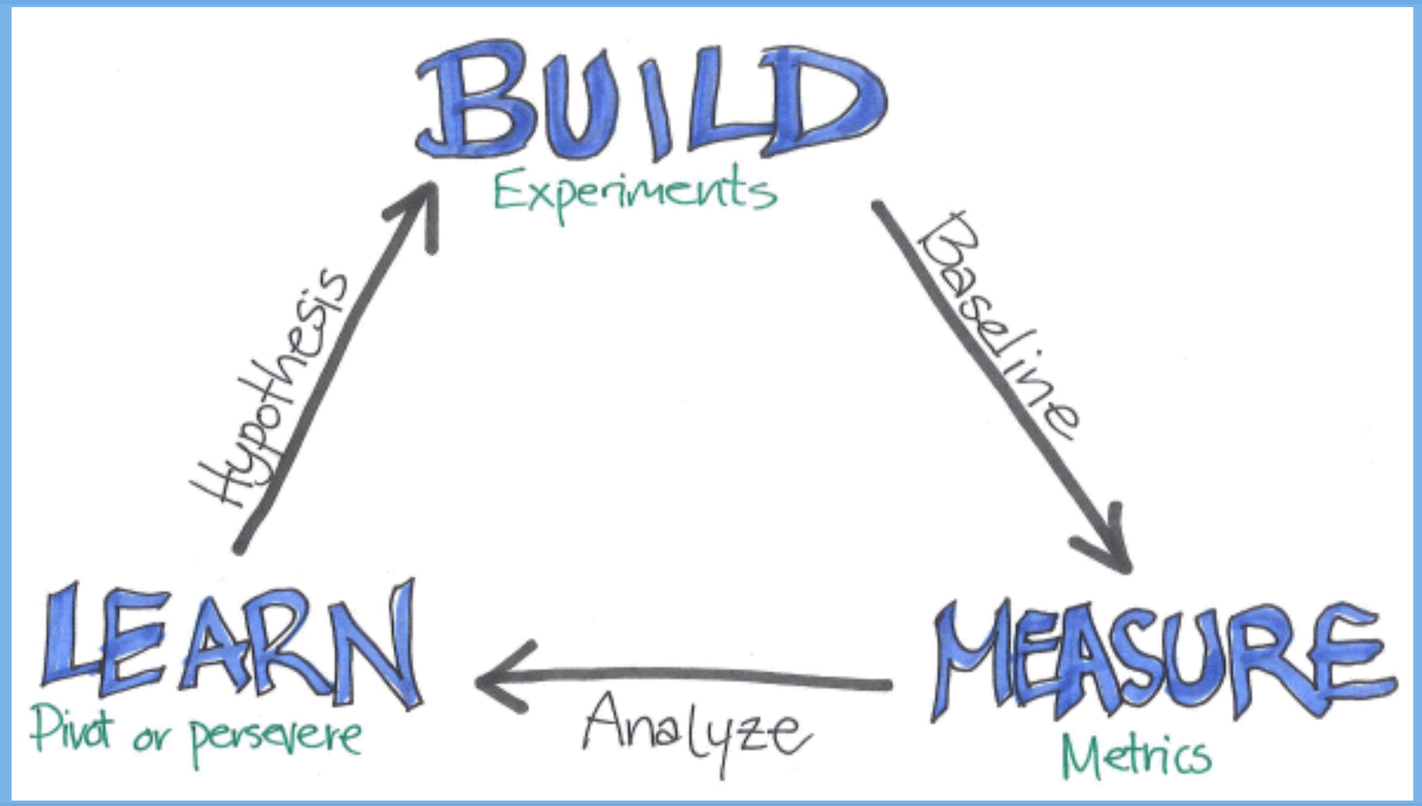
Remember: Reduce Waste & Essentialism

Where's the IT waste? (Dormant Accounts, Config Drift, etc)

Where can you get the biggest ROI of your Hunting time?

Identify features, process, inputs that create successful hunts…
everything else is waste (or could be)!

Remember: Build. Measure. Learn.



Think Big.

Start Small.

Scale Fast.

Be the Hunter Your Environment Needs!

Lean start-up

"Being an entrepreneur is a state of mind, not a job title."

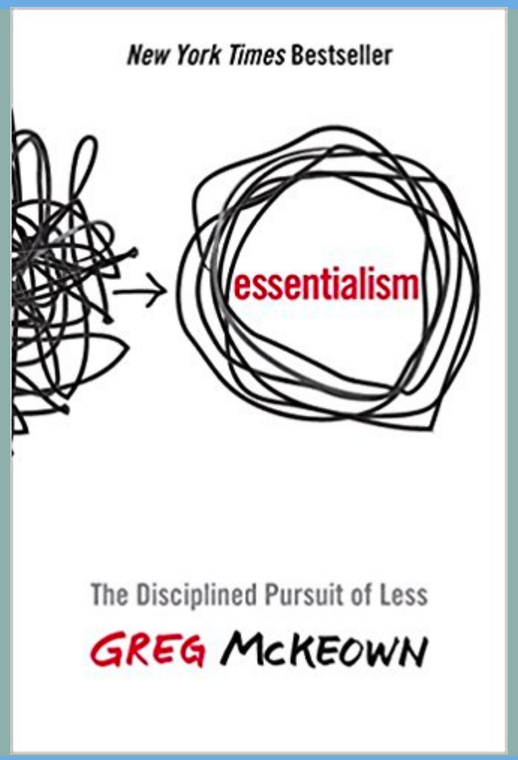
- Guy Kawasaki

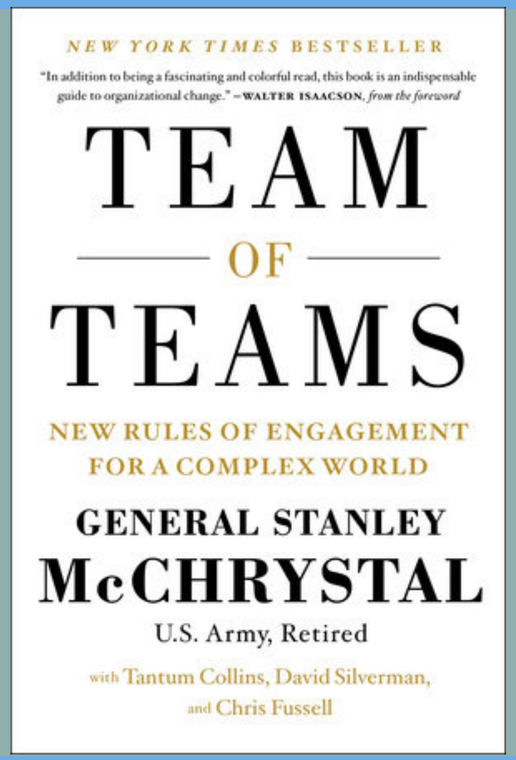
Lean hunting

"Being a hunter is a state of mind, not a job title."

- Ben Johnson (I think?)

Because Who Doesn't Love a Book Recommendation





Today's Goal: TO SPARK CONTEMPLATION

"If you're not embarrassed by your first product you've shipped too late." - Reid Hoffman, LinkedIn Founder

What can you do TODAY to upgrade your hunting?

OBSIDIAN

THANK YOU!

Ben Johnson, CTO

ben@obsidiansecurity.com

@chicagoben | @obsidiansec

OBSIDIAN