RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: STR-R02

BUILDING A DATA DRIVEN SECURITY STRATEGY

Gabriel Bassett

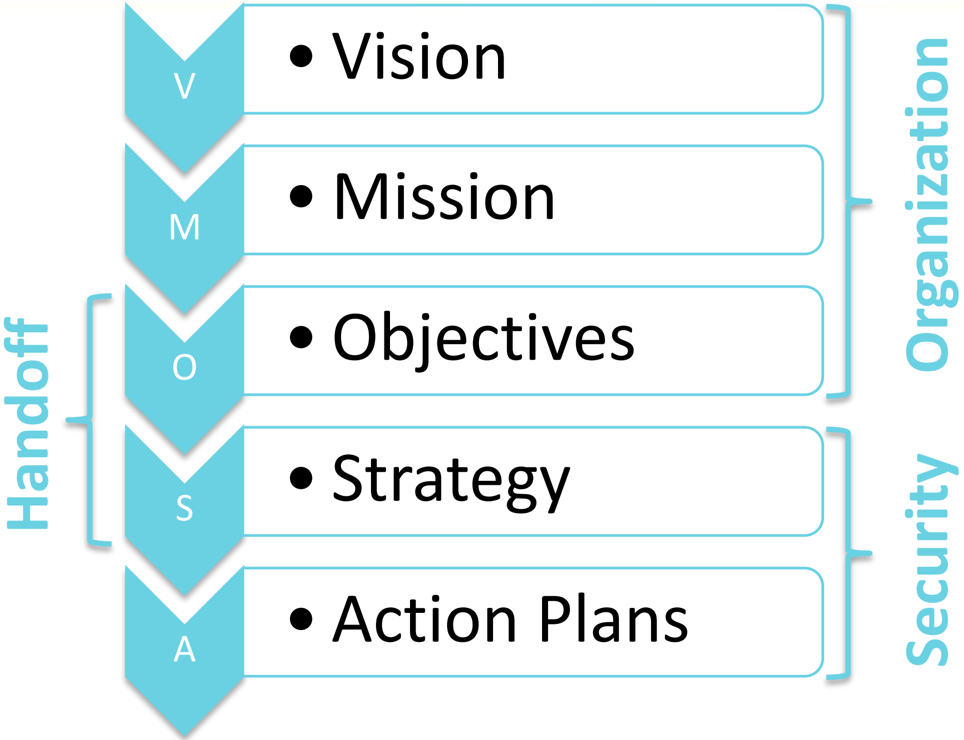
Senior Information Security Data Scientist
Verizon, Data Breach Investigations Report
@gdbassett

Agenda

1. Organization
2. Strategy
3. Measure
4. Data Driven Security Strategy
5. Example Strategies
6. Example Walkthrough
7. Application and Conclusion

WHAT IS A STRATEGY?

VMOSA



V
- Vision

M
- Mission

O
- Objectives

S
- Strategy

A
- Action Plans

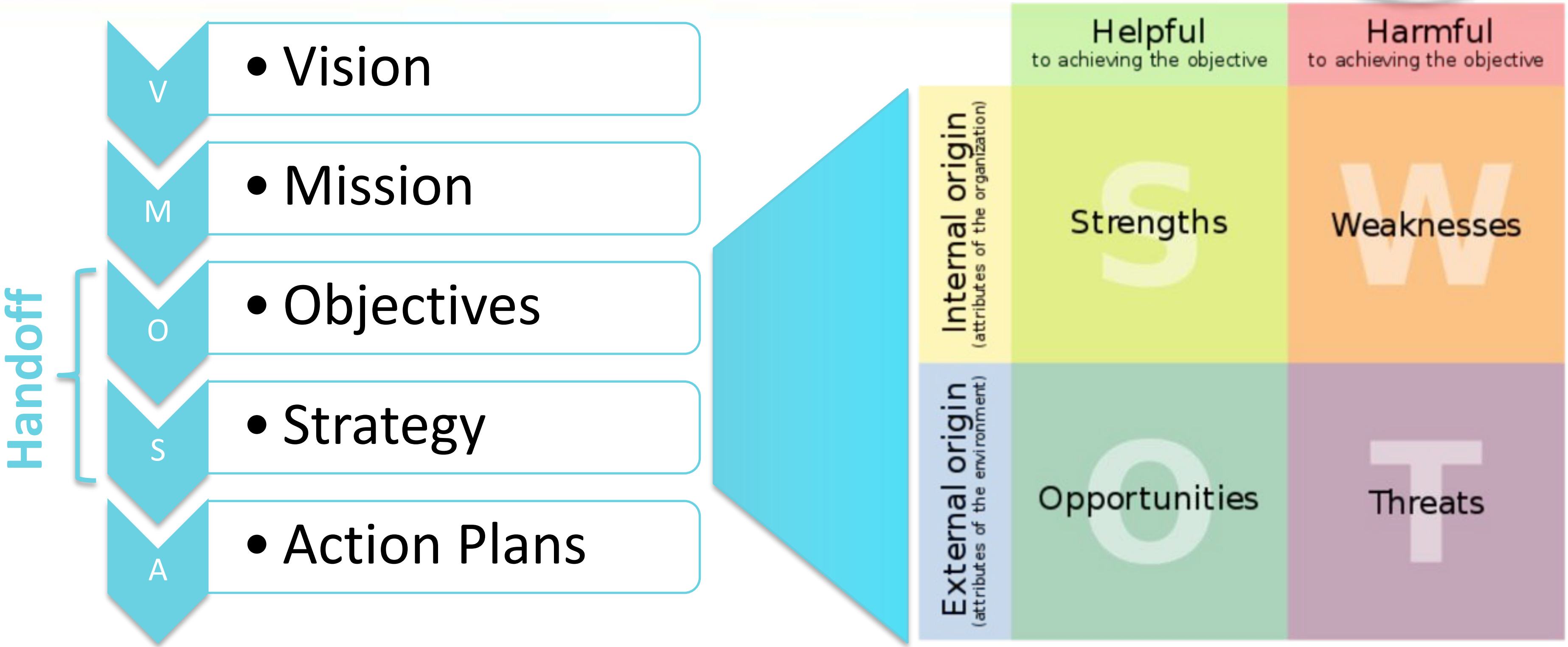
Organization

Security

Handoff

By Denis Fadeev - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=32967868

SWOT Analysis



- V Vision
- M Mission
- O Objectives
- S Strategy
- A Action Plans

	Helpful to achieving the objective	Harmful to achieving the objective
Internal origin (attributes of the organization)	S Strengths	W Weaknesses
External origin (attributes of the environment)	O Opportunities	T Threats

By Xhienne (SWOT pt.svg) [CC BY-SA 2.5 (https://creativecommons.org/licenses/by-sa/2.5)], via Wikimedia Commons

STRATEGY: THE ART OF DEVISING OR EMPLOYING (ACTION) PLANS OR STRATAGEMS TOWARD A GOAL (OBJECTIVE)

https://www.merriam-webster.com/dictionary/strategy

STRATEGY IS HOW YOU CHOOSE PLANS TO MEET YOUR OBJECTIVES

Risk Based Strategy

DATA DRIVEN SECURITY STRATEGY

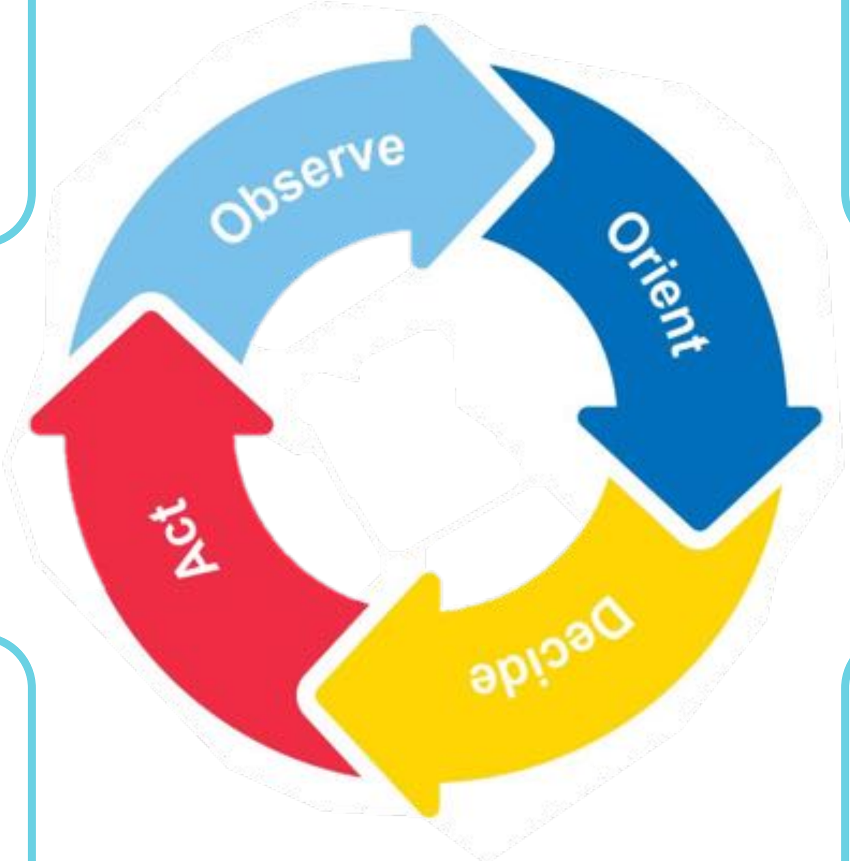
Measures

1. What is my desired outcome?
2. Why is it the right outcome?
3. How do I know the measure predicts this outcome?

Measures

Observations in context of desired Outcome

- VMOSA
- Factor from SWOT



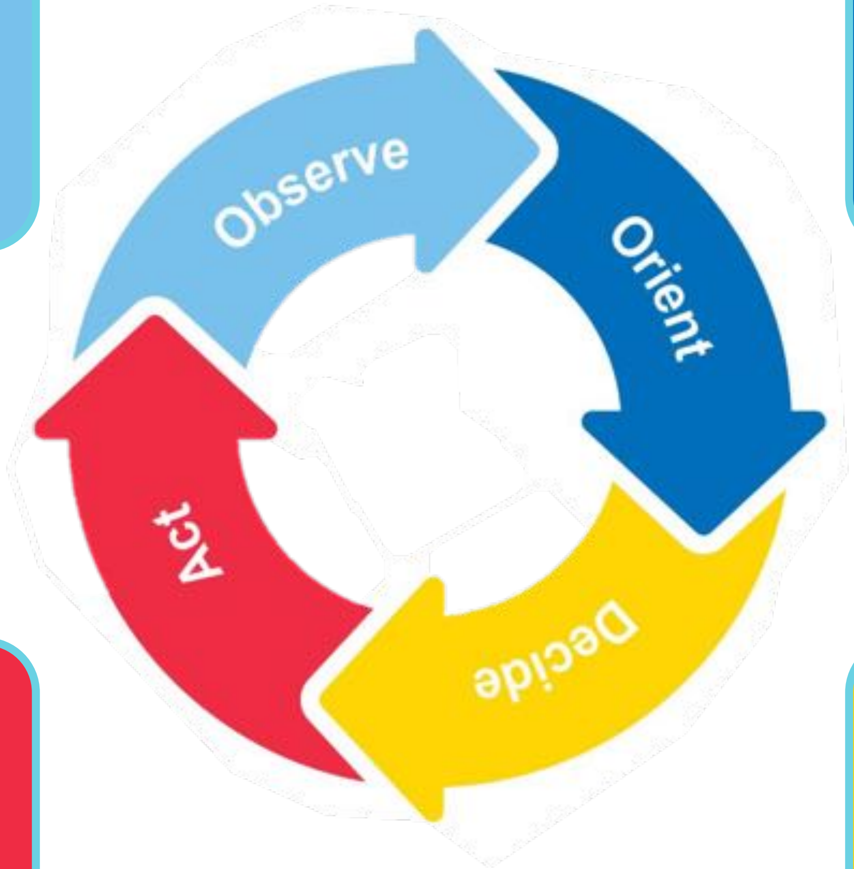
Action Plan
(VMOSA)

Strategy
(VMOSA)

Measures

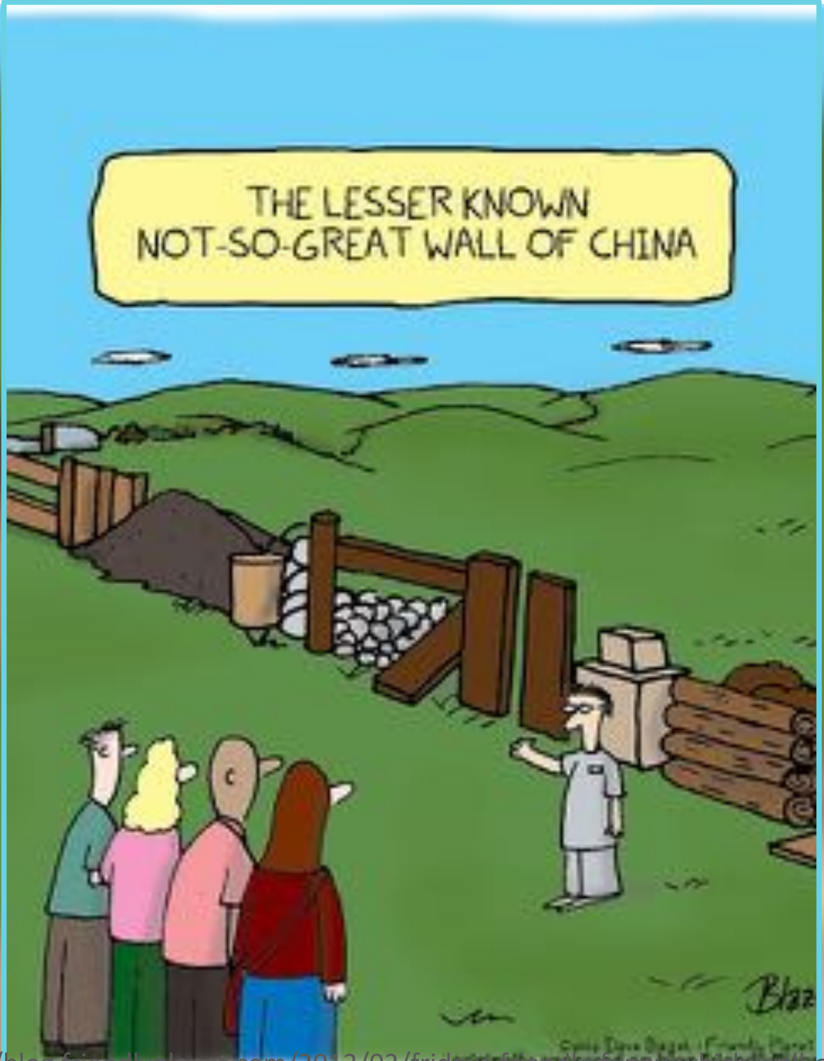
Observations in context of desired Outcome

- VMOSA
- Factor from SWOT



Action Plan
(VMOSA)

Strategy
(VMOSA)



http://blog.friendlyplanet.com/2012/02/fridays-friendly-funny-which-wall-of.html

EXAMPLE STRATEGIES

Strategy: Reactive

Strategy: Support Infosec Ops

Victor Paul (CC BY 2.0) (https://www.flickr.com/photos/victor_paul/8022836740/)

Strategy: Economic Engineering

TimVickers (Own work) [Public domain], https://upload.wikimedia.org/wikipedia/commons/7/71/Alligator_mississippiensis_%282%29%2C.jpg

Strategy: Reduce Infosec Risk

Strategy: Compliance

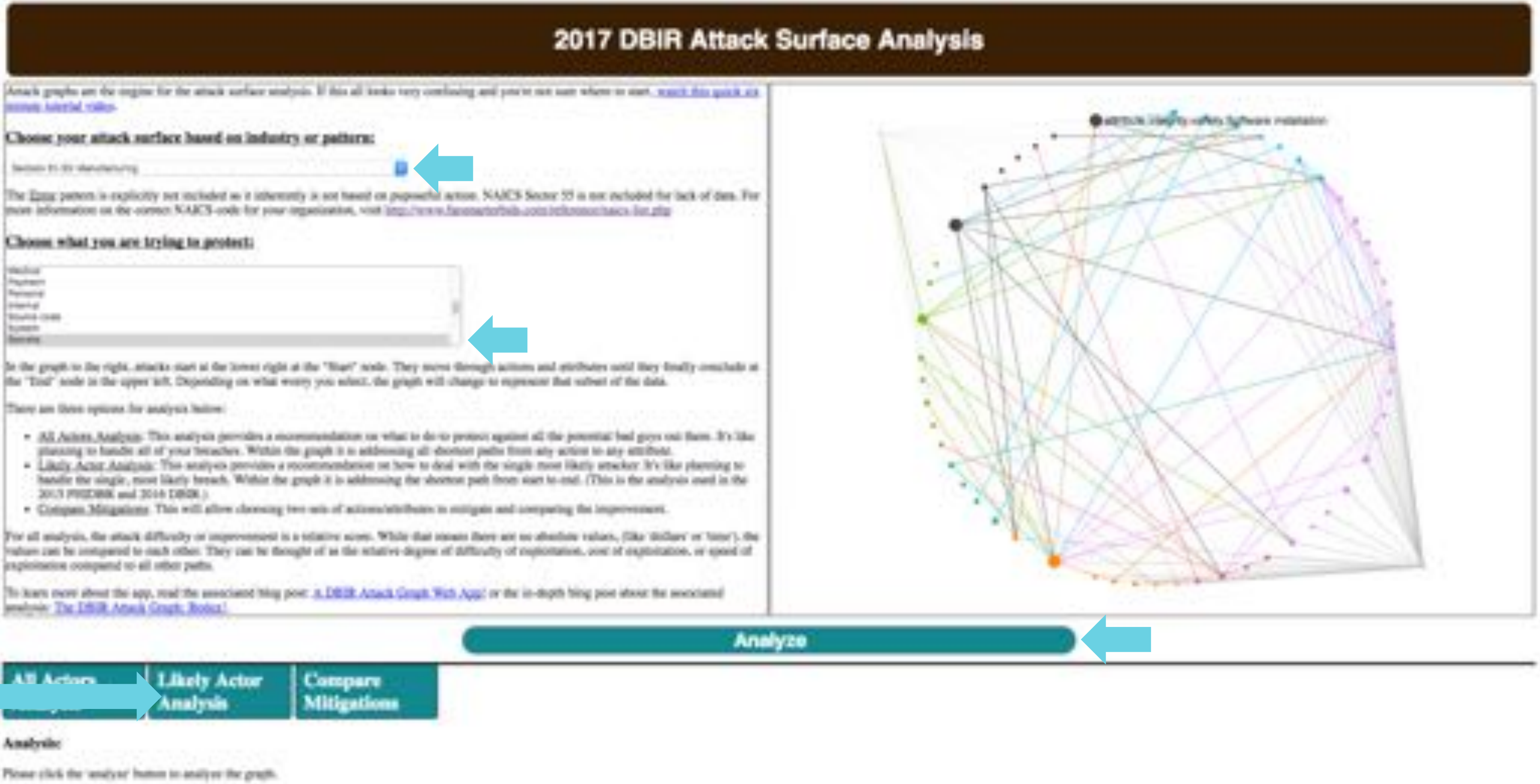
By Pets Adviser from Brooklyn, USA [CC BY 2.0 (http://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons)

Strategy-ish: NIST Framework

By Astris1 (Own work) [CC BY-SA 3.0 (https://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

STRATEGY WALKTHROUGH

Economic Engineering Strategy



2017 DBIR Attack Surface Analysis

Attack graphs are the engine for the attack surface analysis. If this all looks very confusing and you're not sure where to start, watch this quick six minute tutorial video.

Choose your attack surface based on industry or pattern:

Sectors 31-33: Manufacturing

The Error pattern is explicitly not included as it inherently is not based on purposeful action. NAICS Sector 55 is not included for lack of data. For more information on the correct NAICS code for your organization, visit http://www.fasonartorbids.com/reference/naics-list.php

Choose what you are trying to protect:

Medical
Payment
Personal
Internal
Source code
System
Secrets

In the graph to the right, attacks start at the lower right at the "Start" node. They move through actions and attributes until they finally conclude at the "End" node in the upper left. Depending on what worry you select, the graph will change to represent that subset of the data.

There are three options for analysis below:

- All Actors Analysis: This analysis provides a recommendation on what to do to protect against all the potential bad guys out there. It's like planning to handle all of your breaches. Within the graph it is addressing all shortest paths from any action to any attribute.
- Likely Actor Analysis: This analysis provides a recommendation on how to deal with the single most likely attacker. It's like planning to handle the single, most likely breach. Within the graph it is addressing the shortest path from start to end. (This is the analysis used in the 2015 PRIDBIR and 2016 DBIR.)
- Compare Mitigations: This will allow choosing two sets of actions/attributes to mitigate and comparing the improvement.

For all analysis, the attack difficulty or improvement is a relative score. While that means there are no absolute values, (like 'dollars' or 'time'), the values can be compared to each other. They can be thought of as the relative degree of difficulty of exploitation, cost of exploitation, or speed of exploitation compared to all other paths.

To learn more about the app, read the associated blog post: A DBIR Attack Graph Web App! or the in-depth blog post about the associated analysis: The DBIR Attack Graph: Redux!

Analysis:

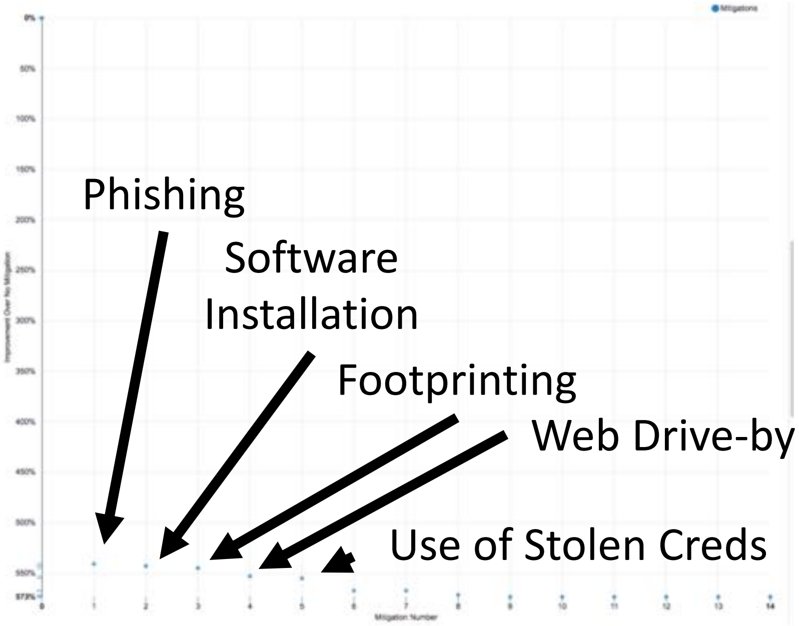
Please click the 'analyze' button to analyze the graph.

http://dbir-attack-graph.infos.ec

Measure risks

Actions and Attributes to Mitigate

- Phishing
- Software Installation
- Footprinting
- Web Drive-by
- Use of stolen credentials



Phishing

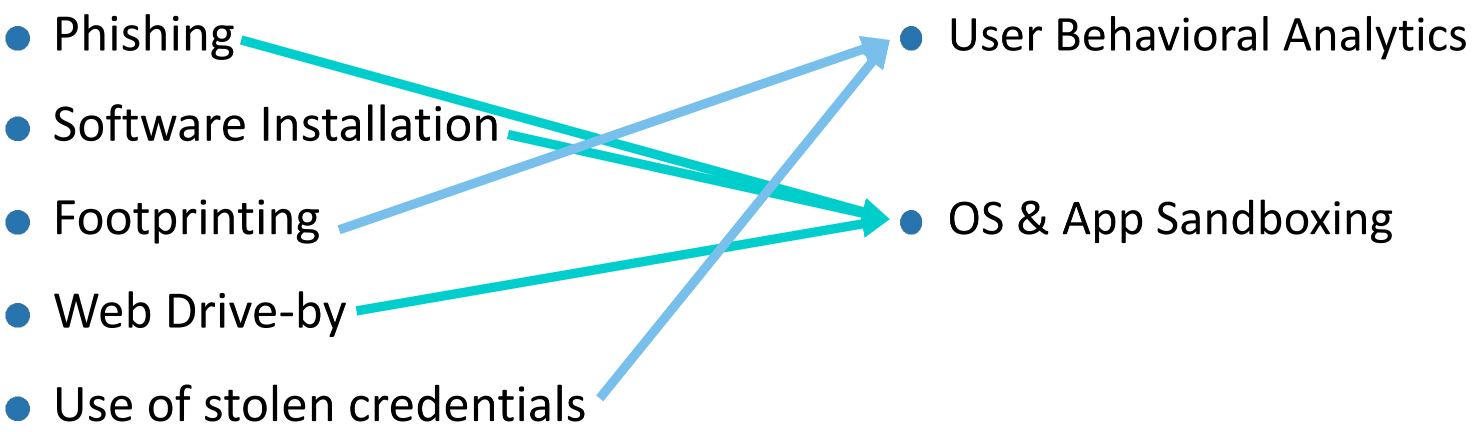
Software Installation

Footprinting

Web Drive-by

Use of Stolen Creds

Map Risks to Plans



Actions and Attributes to Mitigate

- Phishing
- Software Installation
- Footprinting
- Web Drive-by
- Use of stolen credentials

Action Plans or Controls to employ

- User Behavioral Analytics
- OS & App Sandboxing

DOTMLPF-P

Map Plans to Risks

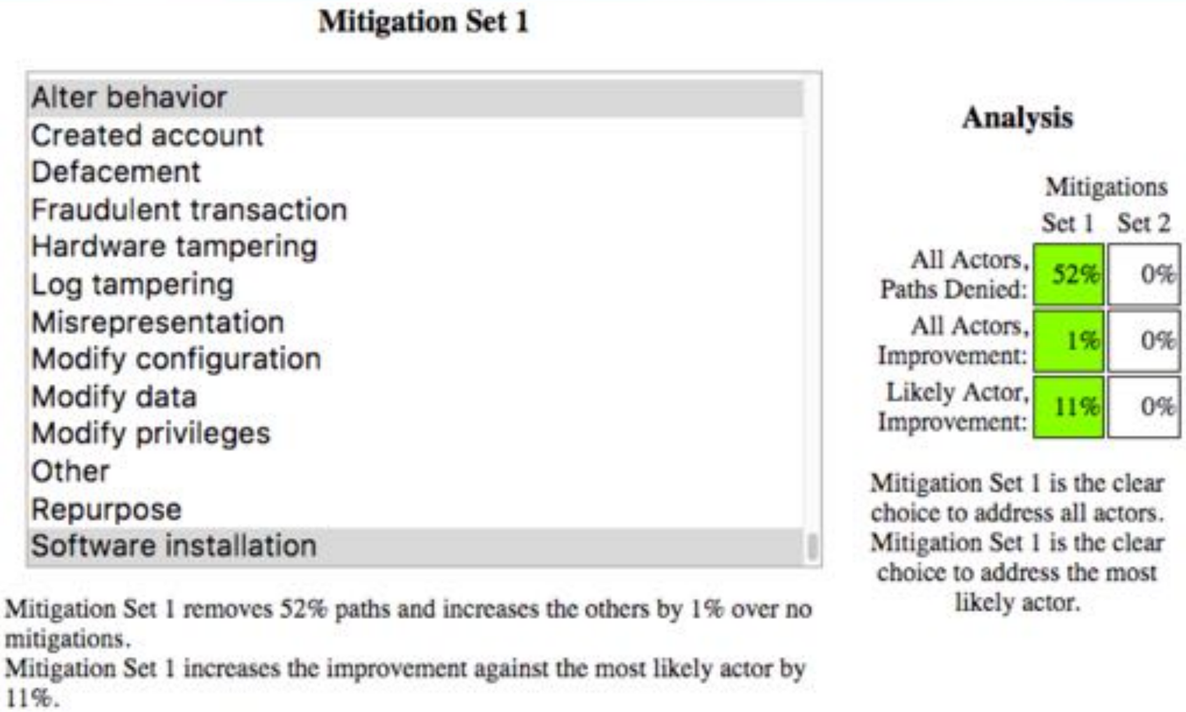
User Behavior Analytics

- Alter Behavior
- Privilege Abuse
- Illicit Content
- Unapproved Workaround
- Abuse of Functionality
- Use of Stolen Creds or Brute force

OS and App Sandboxing

- Phishing
- Malware
  - Web Drive-by
- Hacking (other then credential use)
  - Footprinting
- Software installation

Quantified Improvements



Mitigation Set 1

- Alter behavior
- Created account
- Defacement
- Fraudulent transaction
- Hardware tampering
- Log tampering
- Misrepresentation
- Modify configuration
- Modify data
- Modify privileges
- Other
- Repurpose
- Software installation

Mitigation Set 1 removes 52% paths and increases the others by 1% over no mitigations.
Mitigation Set 1 increases the improvement against the most likely actor by 11%.

Analysis

	Mitigations	
	Set 1	Set 2
All Actors, Paths Denied:	52%	0%
All Actors, Improvement:	1%	0%
Likely Actor, Improvement:	11%	0%

Mitigation Set 1 is the clear choice to address all actors. Mitigation Set 1 is the clear choice to address the most likely actor.

DOING SOMETHING

Next Week

Next Month

The Future

https://pics-about-space.com/future-space-station-wallpaper?p=1

QUESTIONS?

gabriel.bassett@verizon.com

Twitter: @gdbassett

BACKUP