

RSAC[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: HT-T08

The Wolves of Vuln Street: The 1st System Dynamics Model of the 0day Market

Katie Moussouris

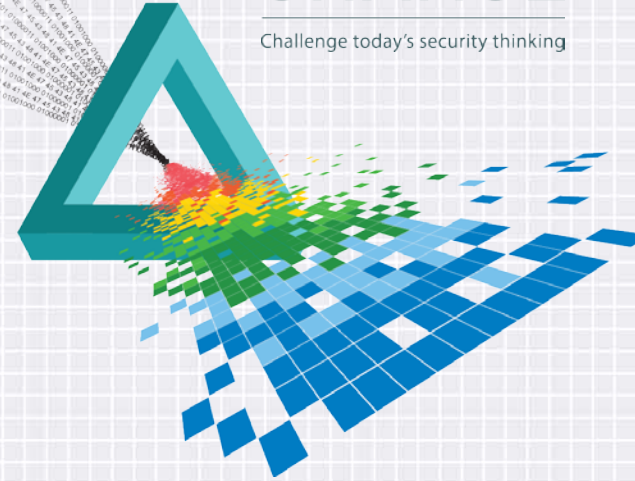
Chief Policy Officer
HackerOne
@K8em0 ← that's a zero

Michael Siegel

Principal Research Scientist
Massachusetts Institute of Technology
@MITsloan

CHANGE

Challenge today's security thinking



Collaborators

- ◆ 0day market system dynamics research funded by **Facebook**

Research Team

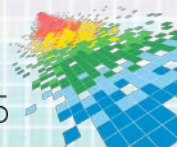
[Dr. Michael Siegel](#), Principal Research Scientist, Sloan School, Massachusetts Institute of Technology

[James Houghton](#), Sloan School, Massachusetts Institute of Technology

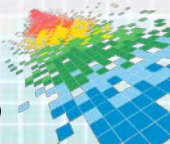
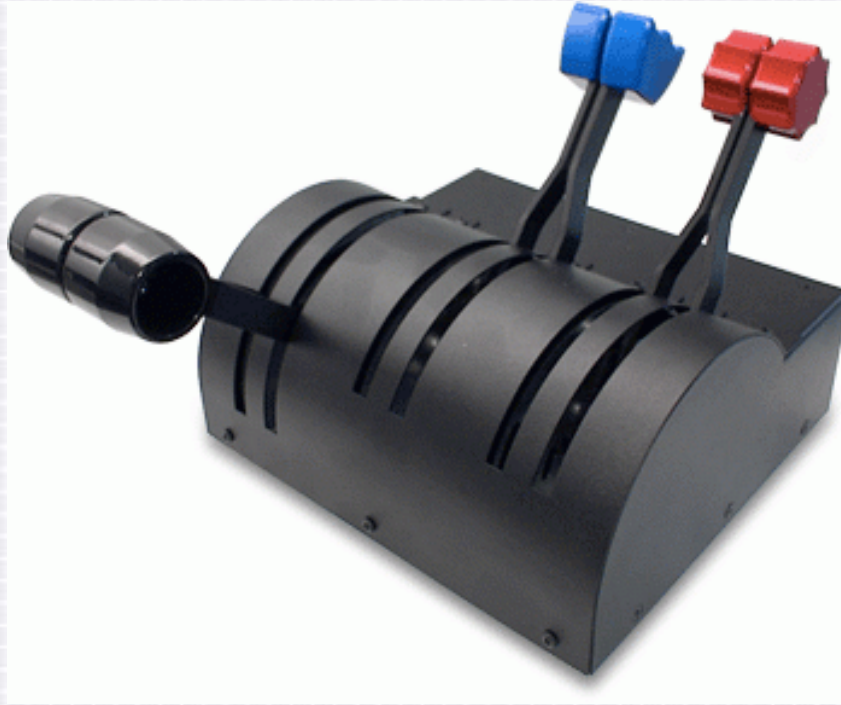
[Dr. Ryan Ellis](#), Harvard Kennedy School

[Collin Greene](#), Security Engineer, Facebook

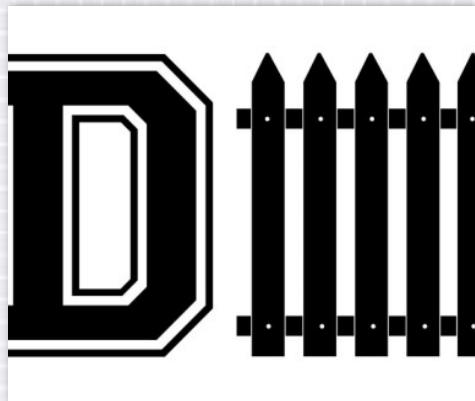
[Katie Moussouris](#), Chief Policy Officer, HackerOne



Why Model the 0day Market?



Myths and Markets – Money Isn't Everything



\$\$\$

DEFENSE



\$\$\$\$\$\$

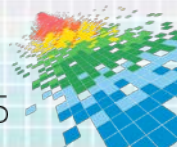
MIXED USE



WAR WERE DECLARED

\$
\$

OFFENSE



WANTED: Dead or Alive – Over \$500,000 PAID

Microsoft's Strategic Bounty Programs:



\$100,000 for new techniques



\$50,000 for new defenses



\$11,000 for IE11 beta bugs

Security TechCenter • Security Updates • Microsoft Security Response Center

Microsoft Security Response Center

The Microsoft Security Response Center (MSRC) works with partners and security researchers around the world to help prevent security incidents and to advance Microsoft product security.



WANTED

New Mitigation Bypass Techniques
\$100,000
Bounty Evolution

Update Lifecycle



Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services.

Security Researcher Engagement

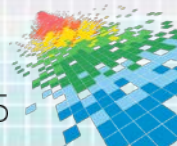


The Bughat team supports collaboration and relationships with security researchers globally to advance Microsoft product security.

Industry Collaboration



Microsoft supports collaboration across the security community so that customers can take timely action to protect their customers while minimizing risk to the ecosystem.



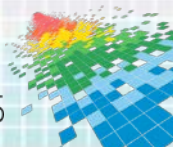
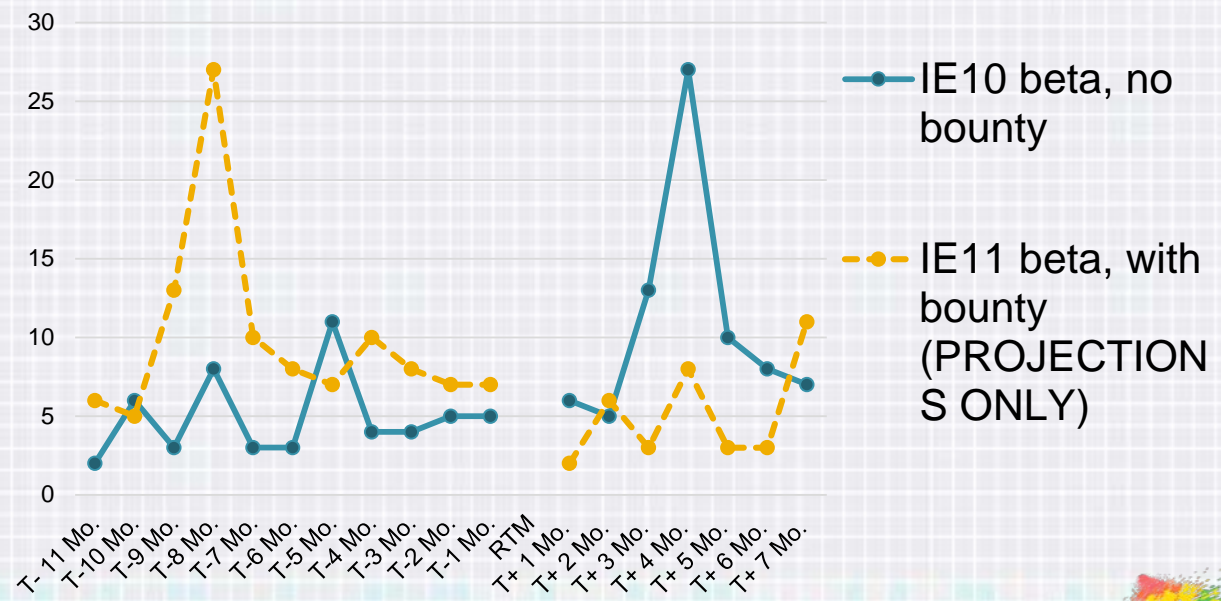
IE Preview (AKA Beta) Bug Bounty: All in the TIMING

◆ James and the Giant Check

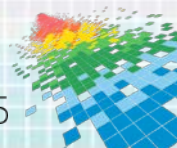
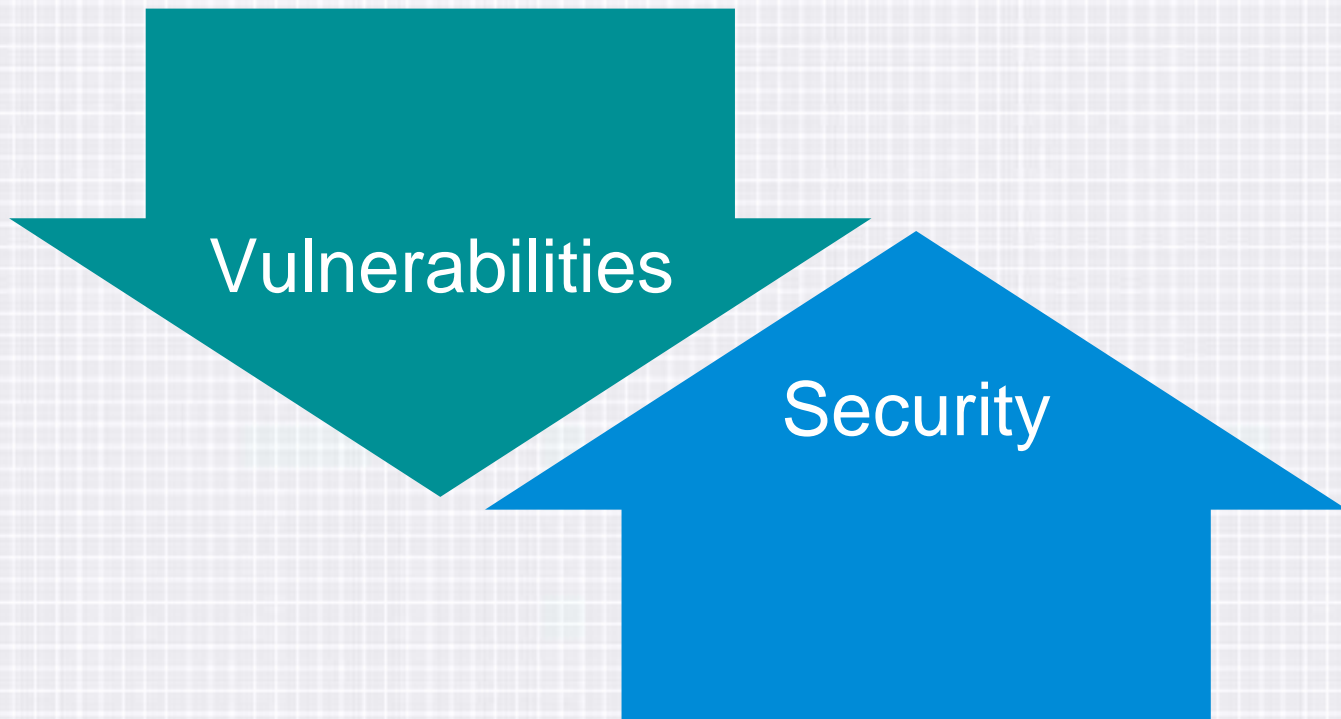
Marketplace Gap:
When Defense is the only game in town

Actual Results:
18 serious security holes

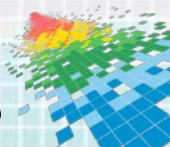
IE10 vs IE11 beta disclosure trends



Vulnerabilities and Security

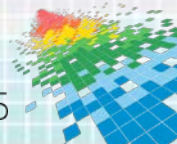


Vulnerabilities: All Different but Still Fruit



Creating a Vulnerability Typology

Vulnerability Characteristics	Quantity of Vulnerabilities ➤	Scarce - Numerous
	Ease of Vulnerability Discovery ➤	Easy - Difficult to Find
	Likelihood of Vulnerability Rediscovery ➤	Low - High
Patching Dynamics	Technical Difficulty of Remediation ➤	Easy - Hard to Fix
	Logistical Difficulty of Remediation ➤	Easy - Hard to Access
	Average Life of a Vulnerability ➤	Short - Long
Market Dynamics	Third Party Market for Vulnerability ➤	Offensive, Defensive, Mixed, Etc.
	Market Size ➤	Small - Large
	Bug Bounty Program ➤	Yes, No
Human Dynamics	Attackers ➤	Criminals, States, Patriots, Etc.
	Researcher Pool ➤	Small - Large
	Attacker Motivation ➤	Political, Financial, Reputational

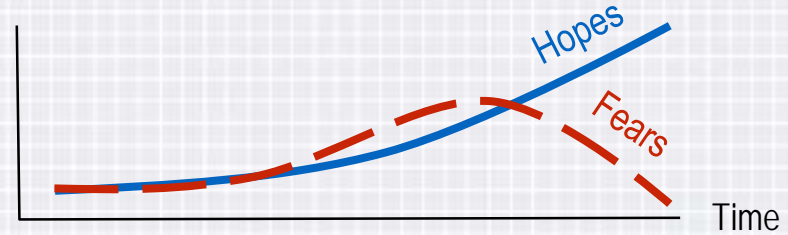


System Dynamics Modeling

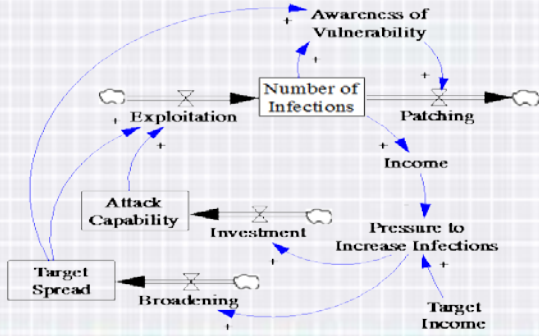
I. Models Complex Human Systems

- ✓ Process Improvement
- ✓ Market Crises
- ✓ Government Stability
- ✓ Software Development

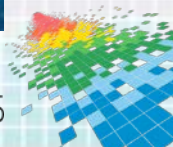
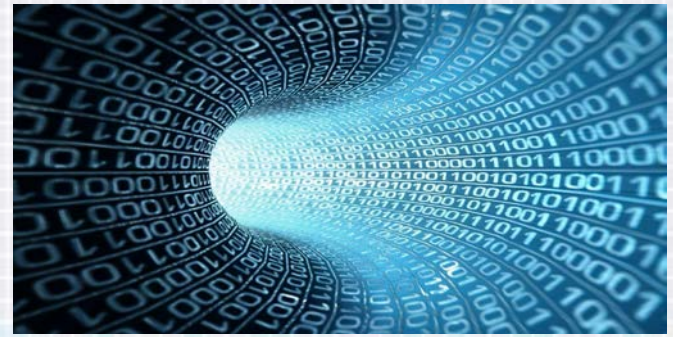
II. Simulates Dynamic, Nonlinear Behavior



III. Formalizes Connection, Causality & Feedback

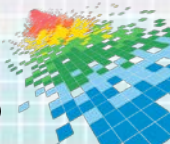


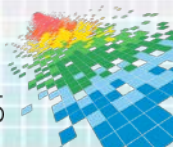
IV. Gives Structure to Data

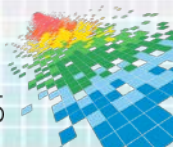
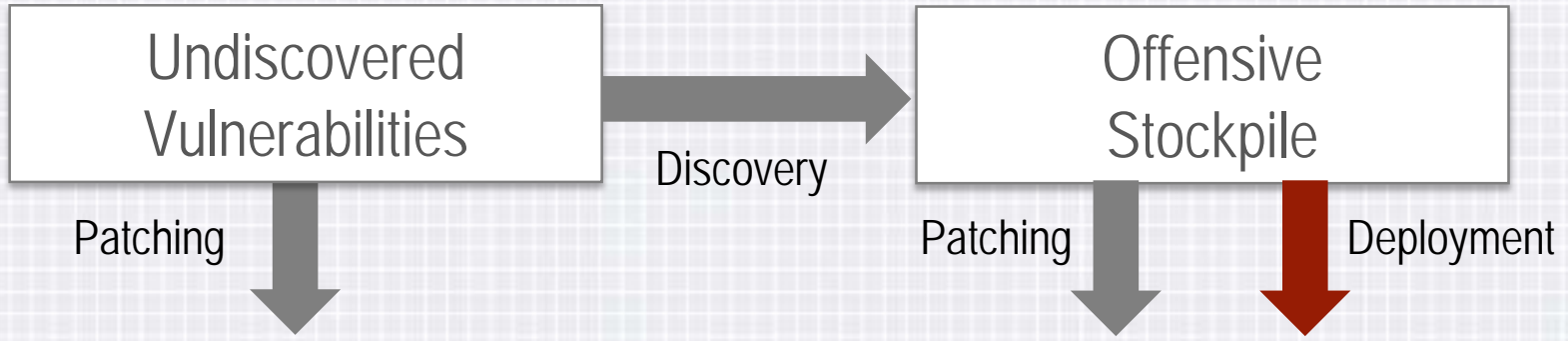


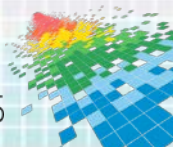
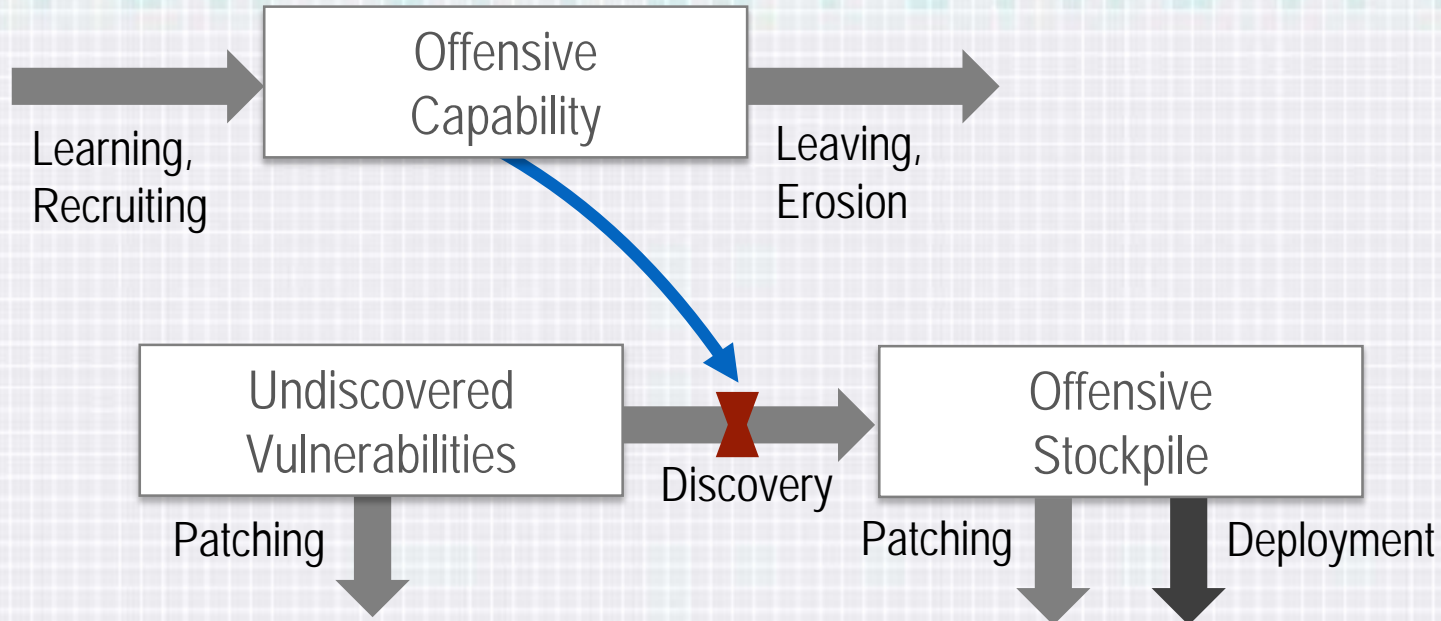
**What policy levers do we have
for reducing vulnerability?**

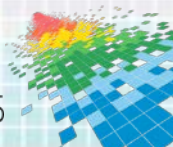
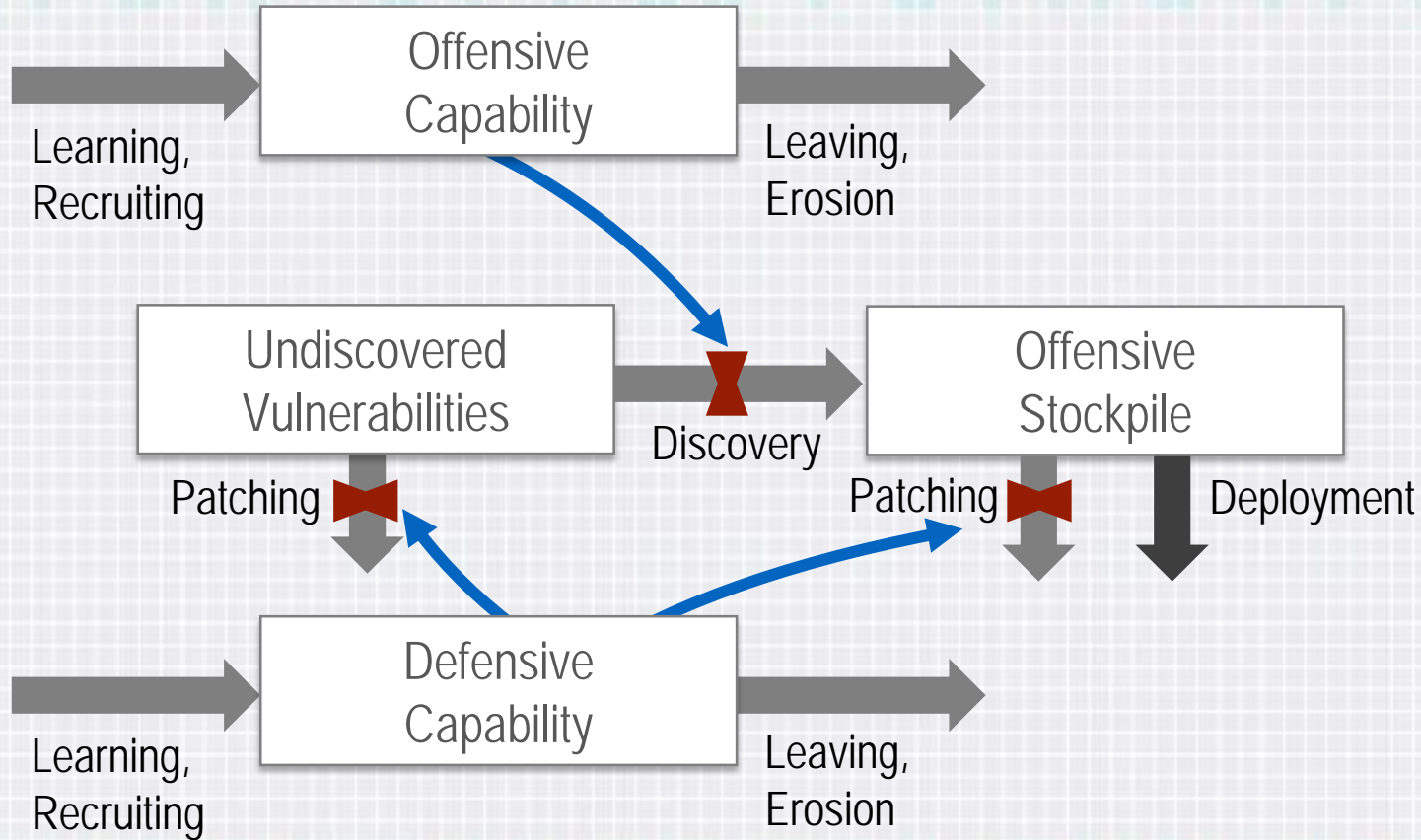
Which has the most leverage?



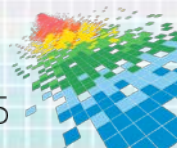
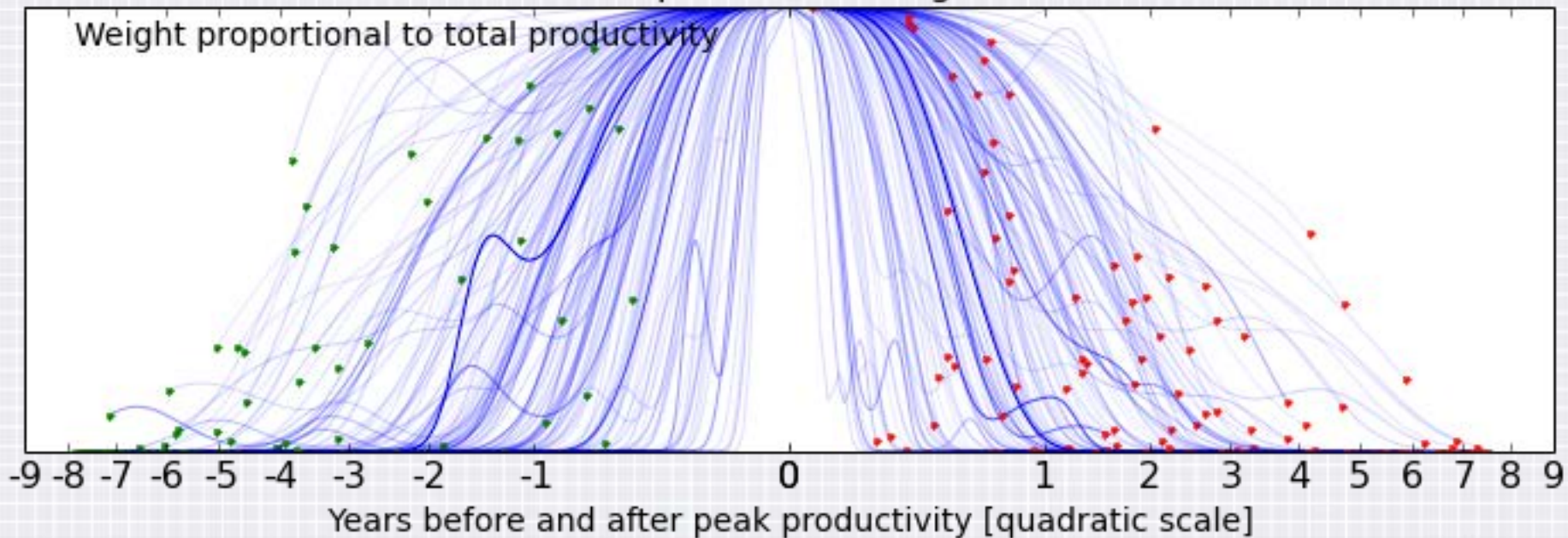


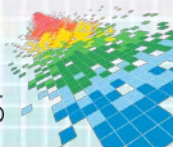
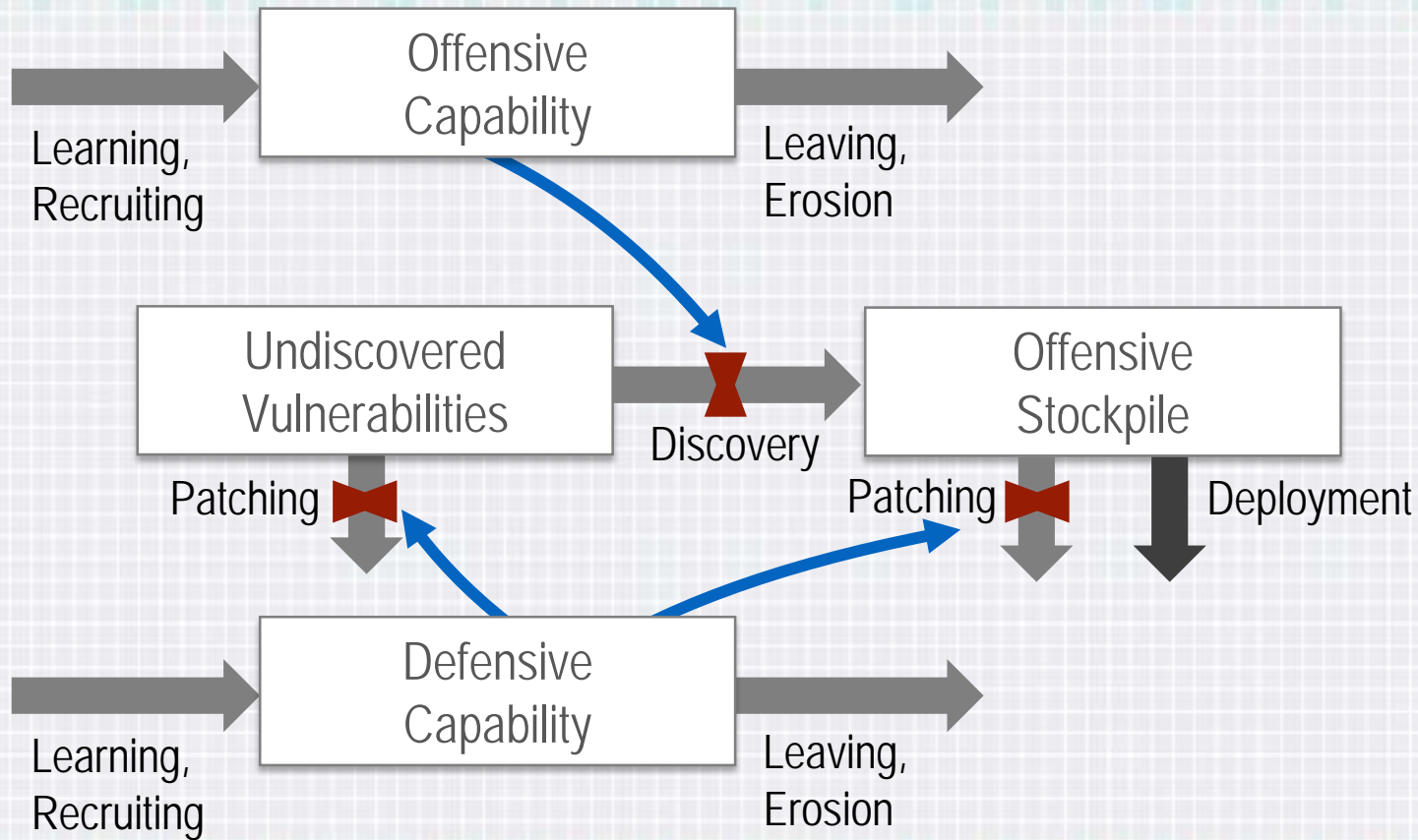


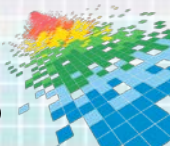
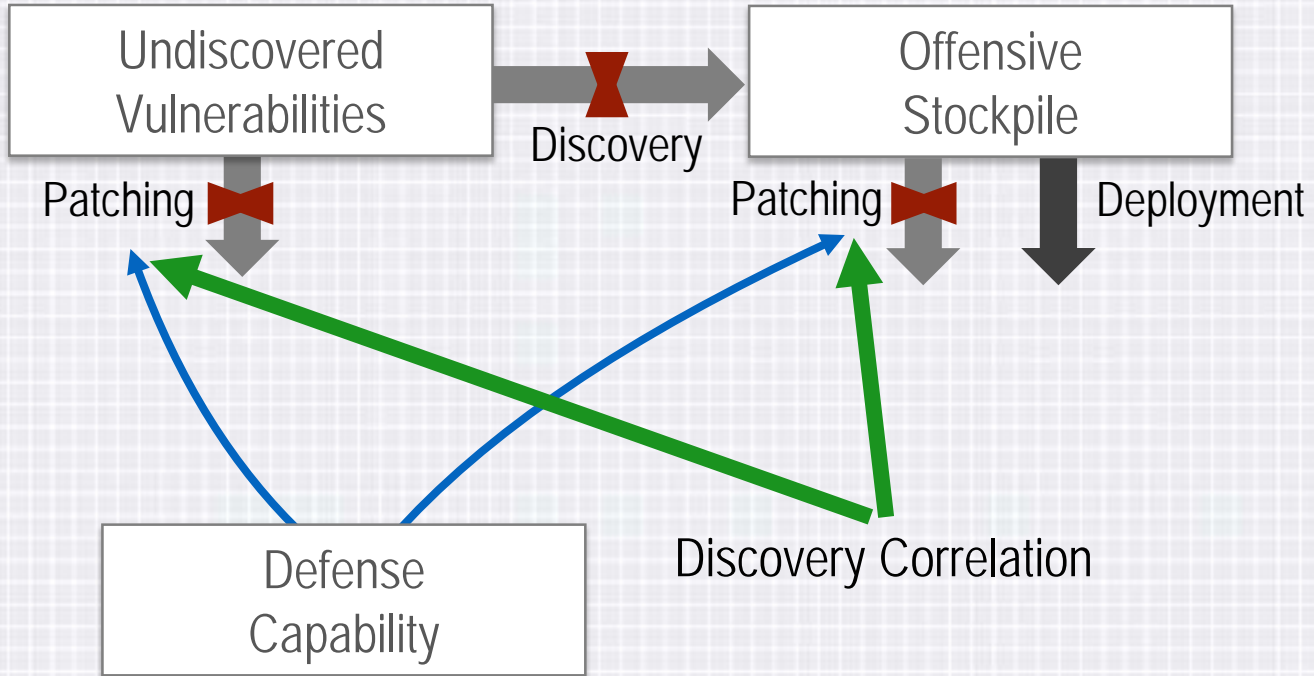




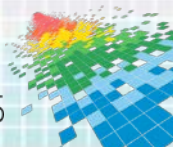
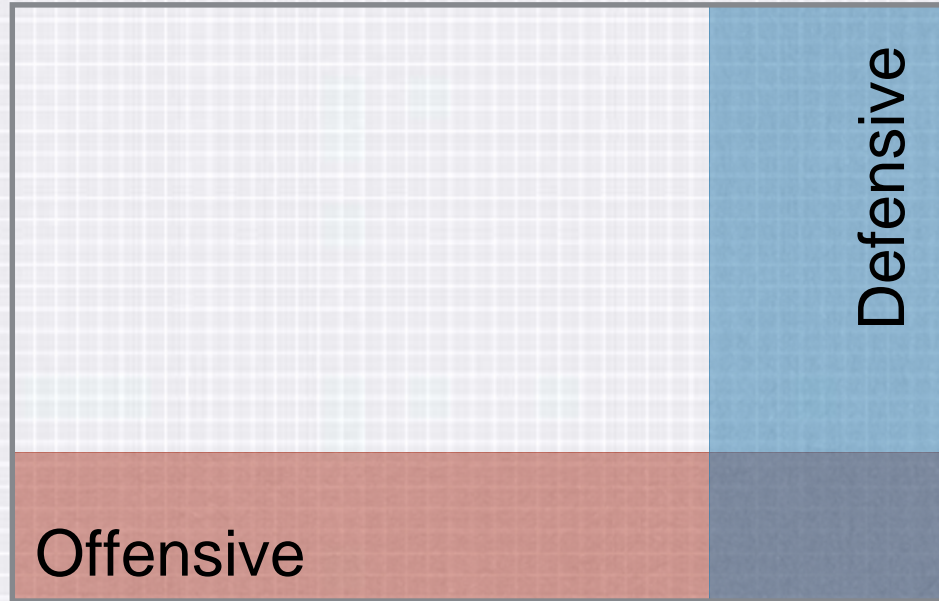
Smoothed, normalized, aligned bug reporting careers of the top 180 MSFT bugfinders



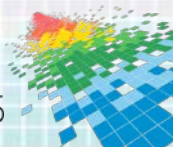
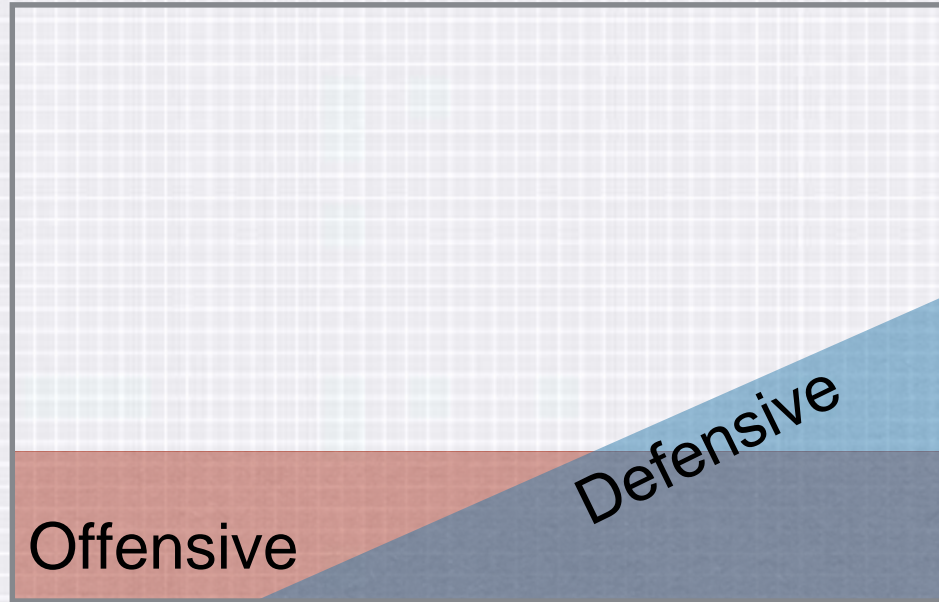




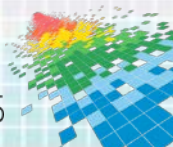
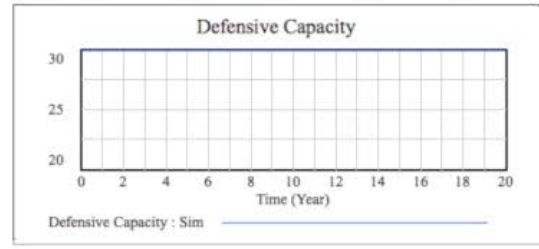
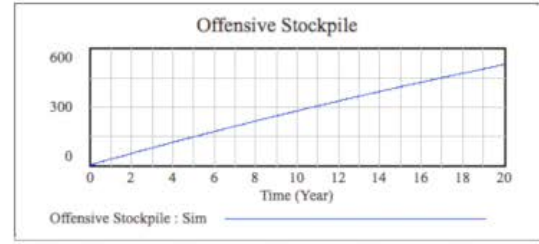
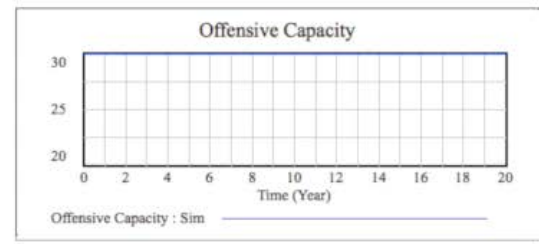
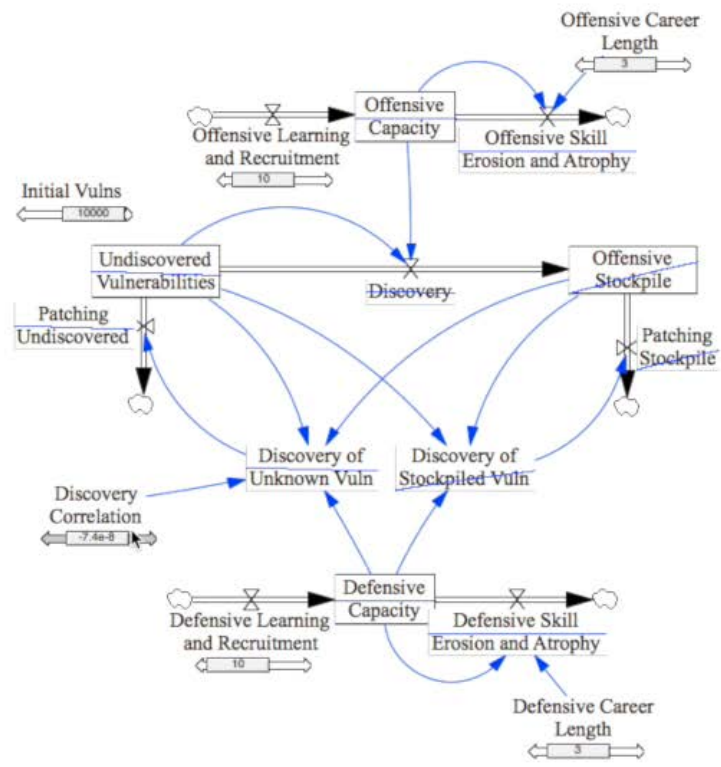
No Correlation



Some Correlation

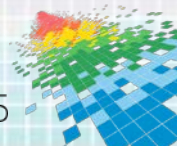


The 0day Market System Dynamics Model



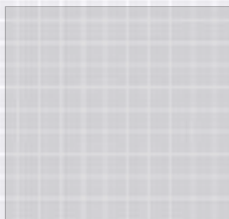
"Bug Collisions" Between Offense & Defense

- ◆ Discovery from offensive stockpile is very sensitive to the correlation. A powerful lever!
- ◆ Defensive capacity development or offensive capacity minimization have different levels of importance depending on the value of the correlation.



How does discovery correlation arise and behave?

The Code Base



Fixed code base

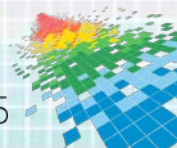
Vulnerabilities



Heterogeneous vulnerabilities

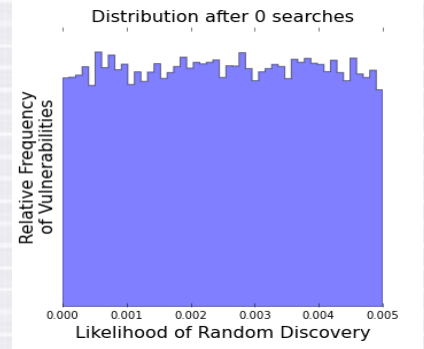
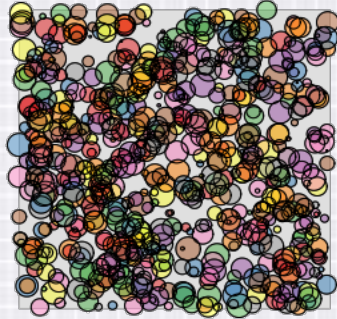


Common techniques between research groups

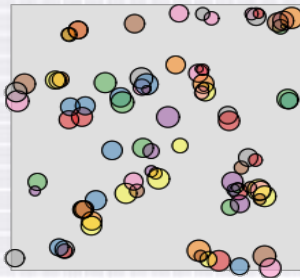


For a young piece of software

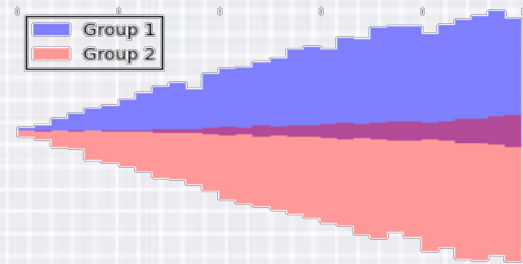
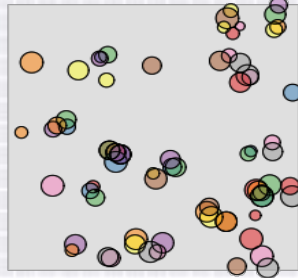
Vulnerabilities in the Code Base



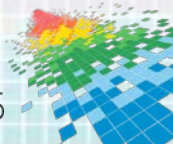
Group 1



Group 2

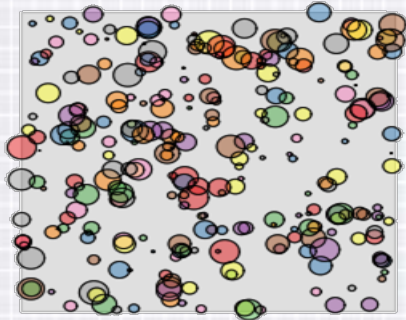


With our model parameters, 9% overlap

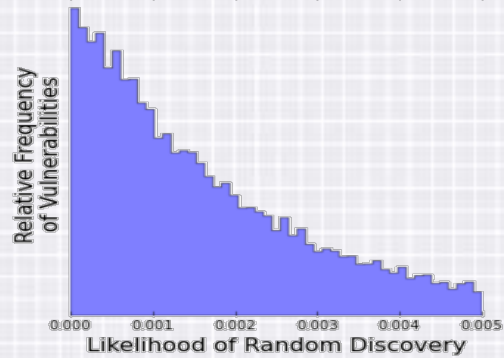


For a hardened piece of software

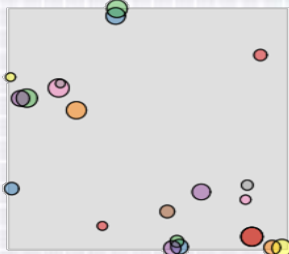
Vulnerabilities in the Code Base



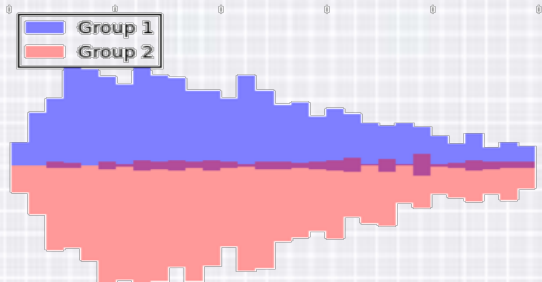
Distribution after 500 searches



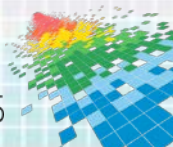
Group 1



Group 2

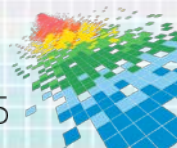


With our model parameters, 0.8% overlap

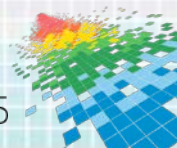


Rate of "Bug Collisions" Varies with Target

- ◆ Correlation can arise naturally due to varied discovery difficulty
- ◆ As software becomes more hardened, expect to see less correlation between discovery groups

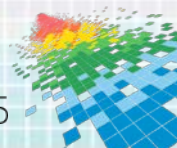


Defenders Scale Best With Tools & Techniques



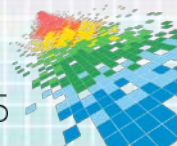
Money Changes Everything

- ◆ Be careful not to create perverse incentives
- ◆ Unintended consequences of draining resources if defense bounties are too high



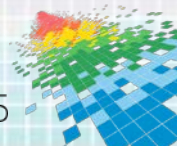
Key Takeaways For Organizations

- ◆ Creating incentives for tools and techniques for vulnerability discovery is a more efficient way for defenders to drain the offensive stockpile
- ◆ Bug bounties are still effective to help find vulnerabilities, especially in less mature software
- ◆ The vulnerability market is not controlled by price alone.



Key Takeaways for Governments

- ◆ Many governments are in the role of both attacker and defender
- ◆ Governments need to broaden the focus of policy debates, it is not just about whether or not to stockpile individual vulnerabilities for offense
- ◆ Governments reap defense gains when they make vulnerability discovery tools and techniques available to defenders.

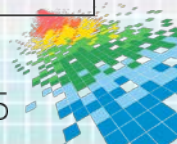


Applying this Research in the Real World

- ◆ Use Incentive programs!
- ◆ Bounty tools and techniques (e.g., fuzzers & tools that help determine exploitability). The most effective way to drain the offensive stock pile.
- ◆ Bug bounties are an effective way to help find vulnerabilities, especially in young software.

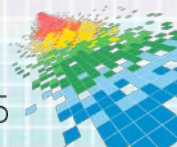
What Are We Doing?

- ◆ The Internet Bug Bounty is offering bounties for tools and techniques this year.
- ◆ We are looking to involve more organizations in our research with MIT

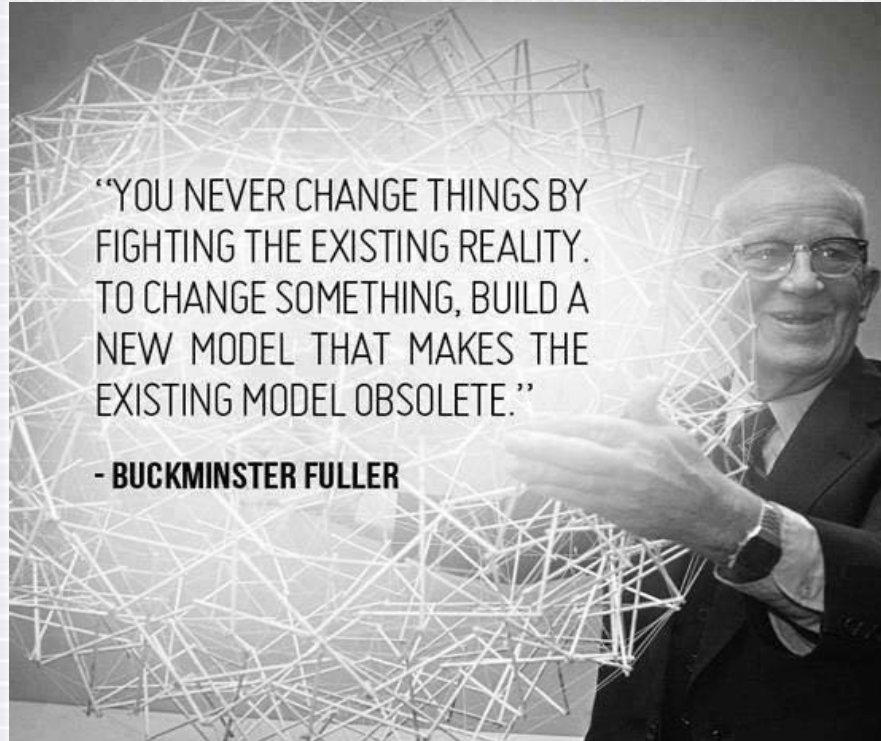


It Has Not Escaped Our Notice...

- ◆ The Wolves of Vuln Street are among us
- ◆ We are studying the dynamics of the pack to make the shepherds of the Internet Defense more effective
- ◆ More models are needed to identify and mobilize other levers besides price in the 0day market



Evolve the Model: All Hands on Deck



“YOU NEVER CHANGE THINGS BY
FIGHTING THE EXISTING REALITY.
TO CHANGE SOMETHING, BUILD A
NEW MODEL THAT MAKES THE
EXISTING MODEL OBSOLETE.”

- **BUCKMINSTER FULLER**

