Social Networking:

The Next Weapon Against Bad Actors

August 22, 2012

GENERAL DYNAMICS
Advanced Information Systems

- David Keener
- David Roberts
- Jonathan Quigg

Beyond Facebook and Twitter…

It’s not about the sites, it’s about the techniques…

Introduction

- Who Are We?
- Our Premise

1. Infrastructure
2. Using Social Networking Technologies Against Bad Actors
3. Thoughts for the Future

Who Are We?

David Keener

GENERAL DYNAMICS
Advanced Information Systems

David Roberts

GENERAL DYNAMICS
Advanced Information Systems

Jonathan Quigg

DATA TACTICS CORPORATION

We're engineers,
web experts,
and data manipulators

Our Premise

The Cyber Security Community can achieve major benefits from a widely used "Indicators Sharing Platform"…

- That facilitates knowledge sharing
- That leverages social networking techniques to deliver synergistic effects

Social Networking Techniques Like…

- Crowd-Sourcing
  - Leveraging community expertise
- Reputation Ranking
  - Highlighting the most useful analysis
- Predictive Recommendations
  - Showing you what you need to know
- Increased Information Dissemination
  - Sharing info the community already has

We Can Design the System…

Right in front of you…

Right now…

Part 1. Infrastructure

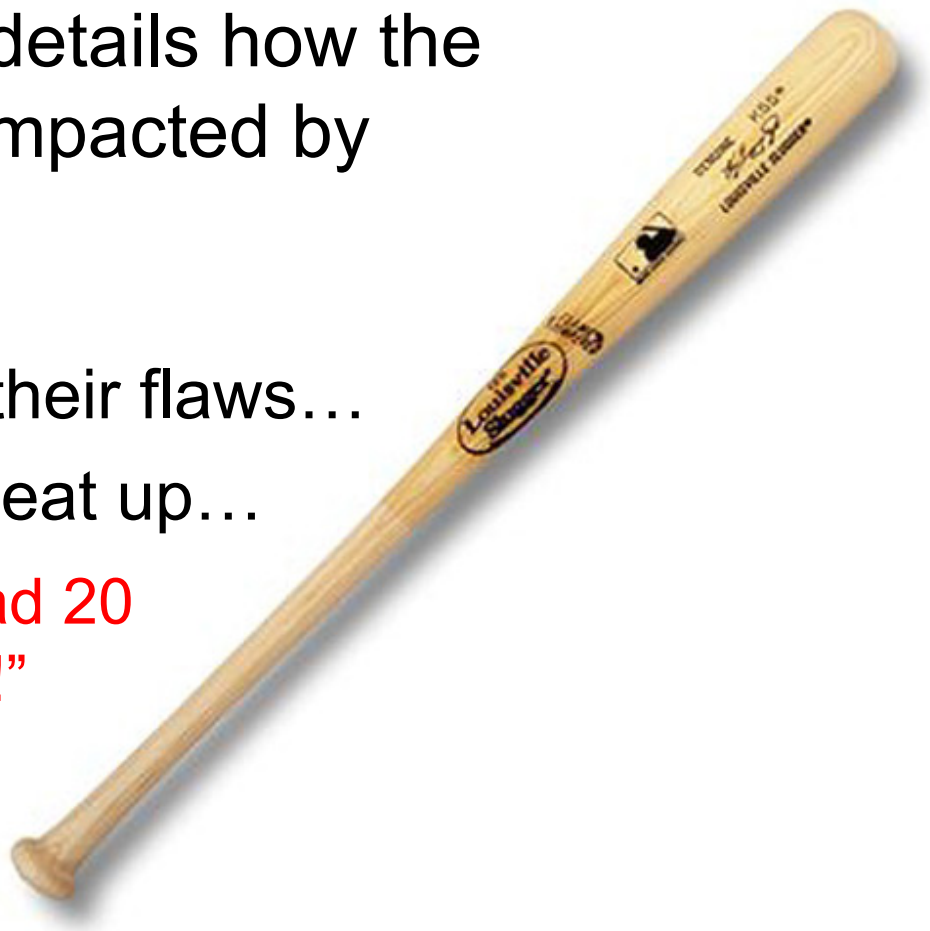
Our Baseline Needs To…

- Facilitate knowledge sharing
- Solidify our terminology
- Support critical security features

The Problem with Knowledge Sharing

Incident – A report that details how the reporter was adversely impacted by malware.

- Nobody likes to show their flaws…
- Nobody wants to get beat up…
  - "Your organization had 20 incidents last month!"

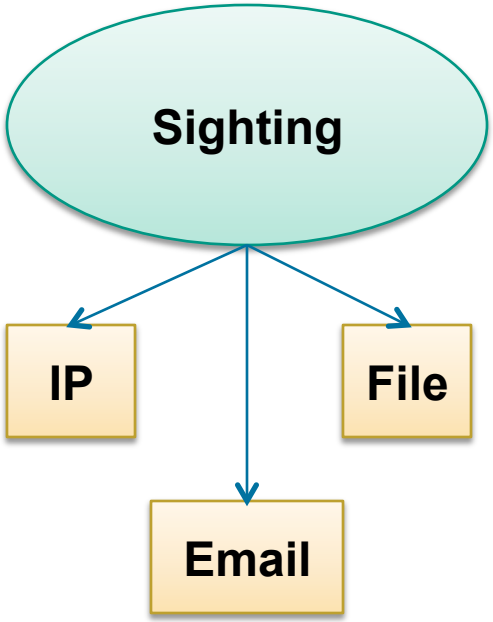


So, we need a new term…

Terminology

- **Indicator** – An object that potentially indicates the presence of malware: Ex. – Files, Emails, IP Addresses, Domain Names, etc.

- **Sighting** – A group of indicators believed to be closely related

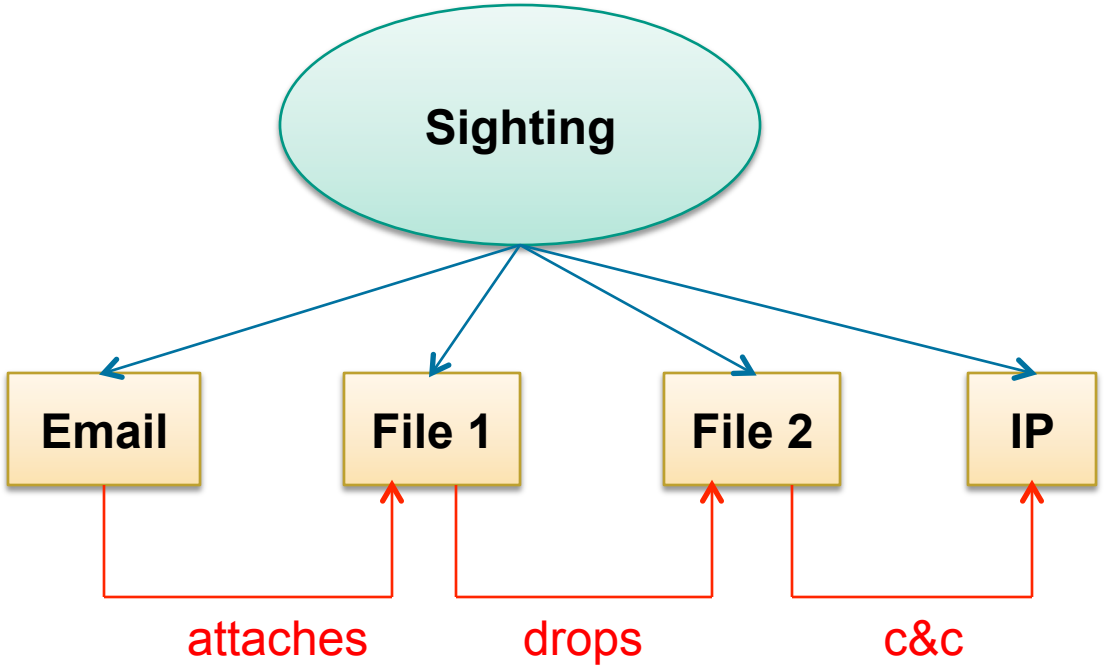


Sightings vs. Incidents

An Incident is certainly a Sighting,
but a Sighting is not necessarily
an Incident!

Relationships

A relationship describes how two indicators are related to each other.



Security Infrastructure

- Authentication
- Roles
- Access Control
- Dissemination Guidance

Plus, behind the scenes…

- SSL
- Network Security
- Auditing

Roles: What Can I Do?

- What features do I have available to me?
- Can I view objects?
- Can I create or edit objects?
- Can I delete objects?
- Can I perform searches?
- Can I see metrics?
- Can I create user accounts?

Access Control: What Can I See?

- Indicators
  - Can be “published” to one or more communities
- Users
  - Can belong to one or more communities
  - Can see an indicator if it’s published to a community that a user belongs to
- Sightings
  - Sightings inherit the communities of their indicators
  - If you can see an indicator, you can see the sighting

What Can I Do With What I Can See?

Is there an official designation?

- FOUO/SBU
- Classified/Unclassified

Is there any other guidance?

- Traffic Light Protocol

Traffic Light Protocol

- Red
  - Can only be shared with involved parties
- Amber
  - Own org. need to know; and only as far as needed to take necessary actions
- Green
  - Peers & partner orgs in sector, but not public
- White
  - Public

From US-CERT: http://www.us-cert.gov/tlp/

Optional Anonymity

- The system needs to know who users are
- The system needs to know organizations

- Optionally, users could have “handles”
  - Ex: “cyberspy01”
- Optionally, orgs could have generic descriptions
  - Ex: “Government Agency”

Our Starting Point

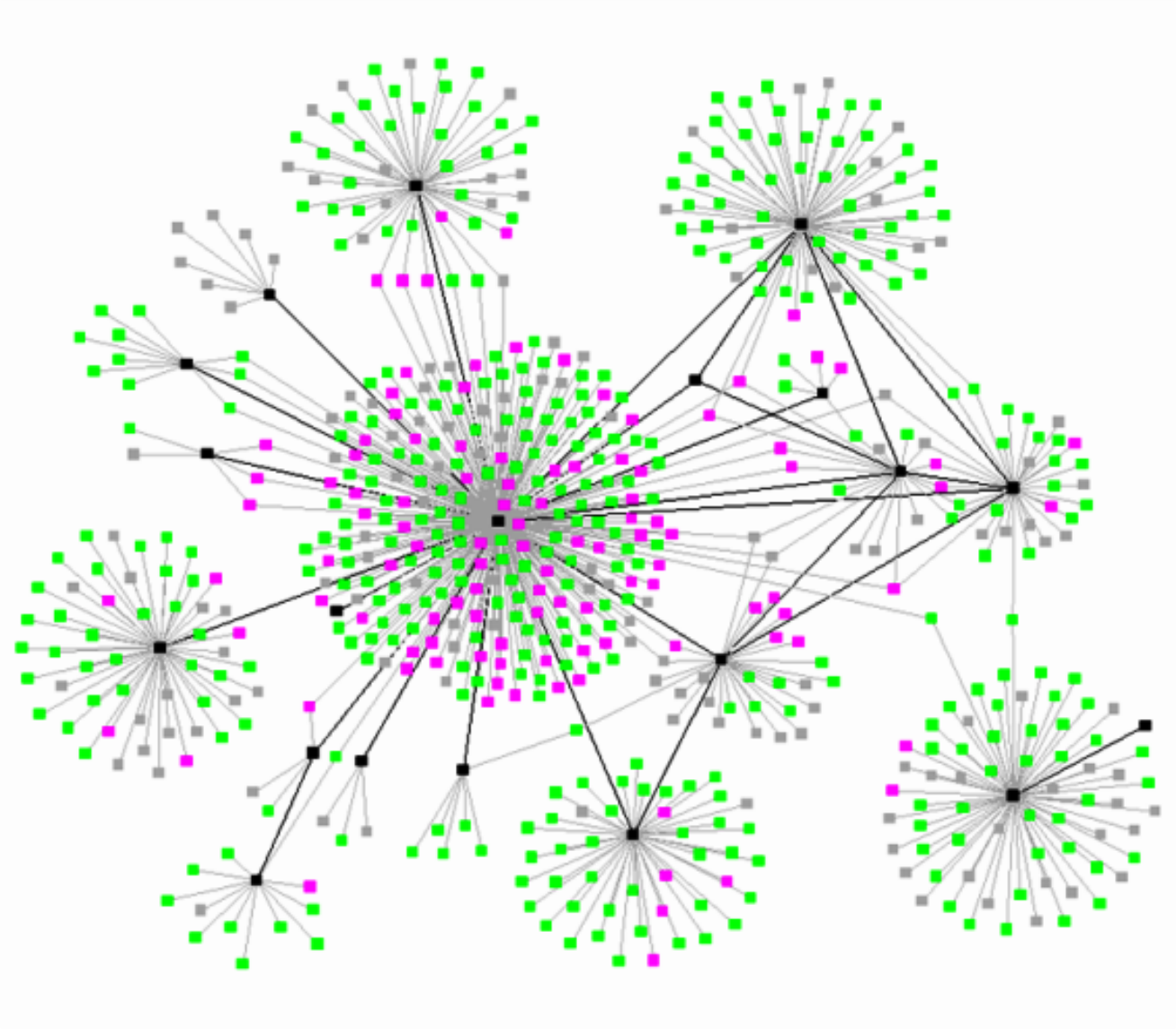
- A system that can store sightings, indicators and relationships
- Users with well-defined roles
- Fine-grained access control

We Have Done This…

- We've built a system like this
- We have the experience

Now, we're going to take it to the next level

Part 2: Using Social Networking Techniques



Leveraging the Community

- Make the system widely available
- Allow users to enter sightings/indicators
- Allow users to comment on sightings/indicators

Before We Go Further…

Let's explore interactivity in a really simple "community" that we're all familiar with…

The Couch Potato Community

You might think that TV is a non-interactive medium

- The TV plays…
- You watch…
- No real interactivity

Except for the Remote

Television Exists to Sell a Product

- **We** are the product
- Advertisers are the customers

(Alert: Product Substitution Detected)

Even the very limited activity of TV viewers provides great value…

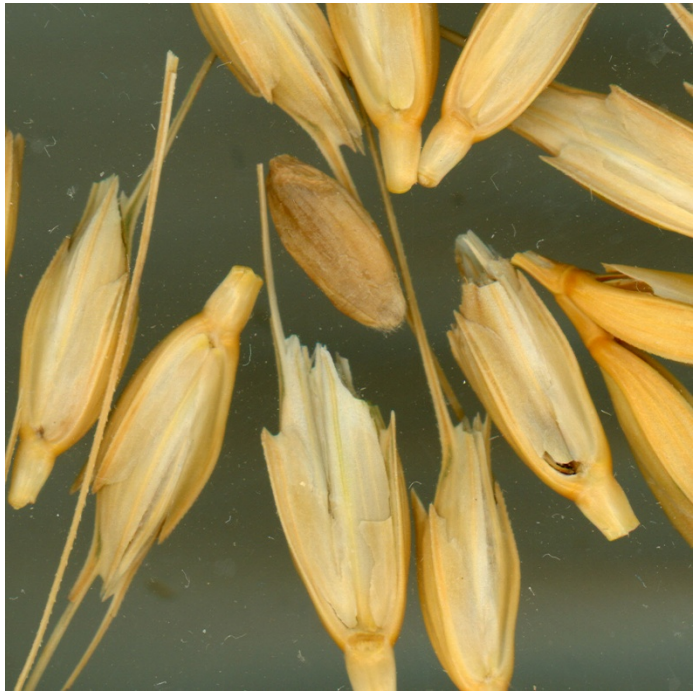
Web Apps Facilitate Interactivity

- Can support interactivity in many ways
- Can generate a lot of valuable info

Let's think about the **impact of interactivity** on our app

Mining the Content

- Some indicators and sightings will be useful
  - Some not so useful
- Some comments will be good
  - Some will be bad

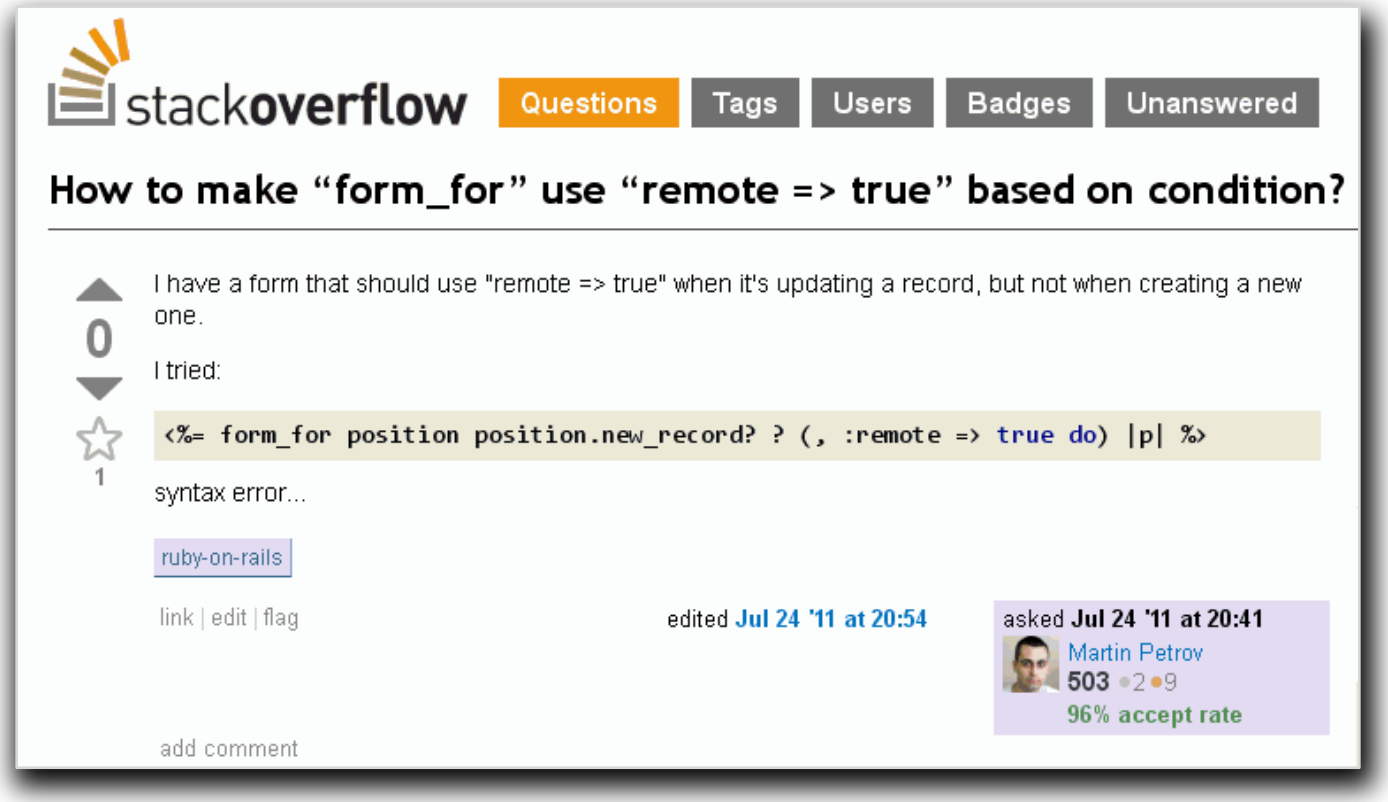


Grain and Chaff

Let the community evaluate them

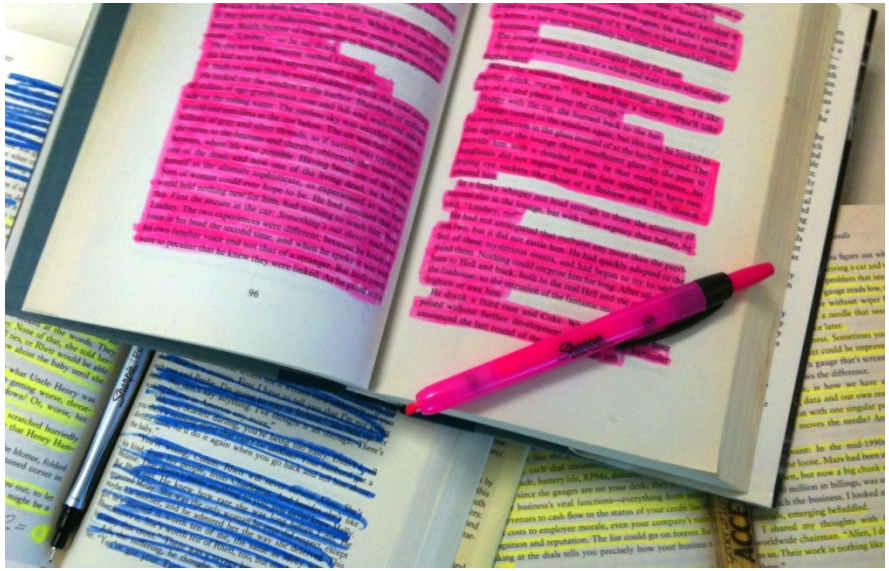
Voting

- Up Vote: Useful & Relevant
- Down Vote: Not Useful



Comment Relevancy Threshold

- If enough people think a comment is irrelevant
  - Hide it
- Keeps relevant data in front of the community
- Helps promote “information density”



What About Sightings & Indicators?

- Can’t hide them…they are real reports
- Voting can affect relevancy
- Higher relevancies emphasized in search results
- Voting results shown throughout the app

To Summarize…

- We've let users enter Sightings & Indicators
  - And vote on them
- We've let users enter comments
  - And vote on them

We're doing a reasonably good job of evaluating content

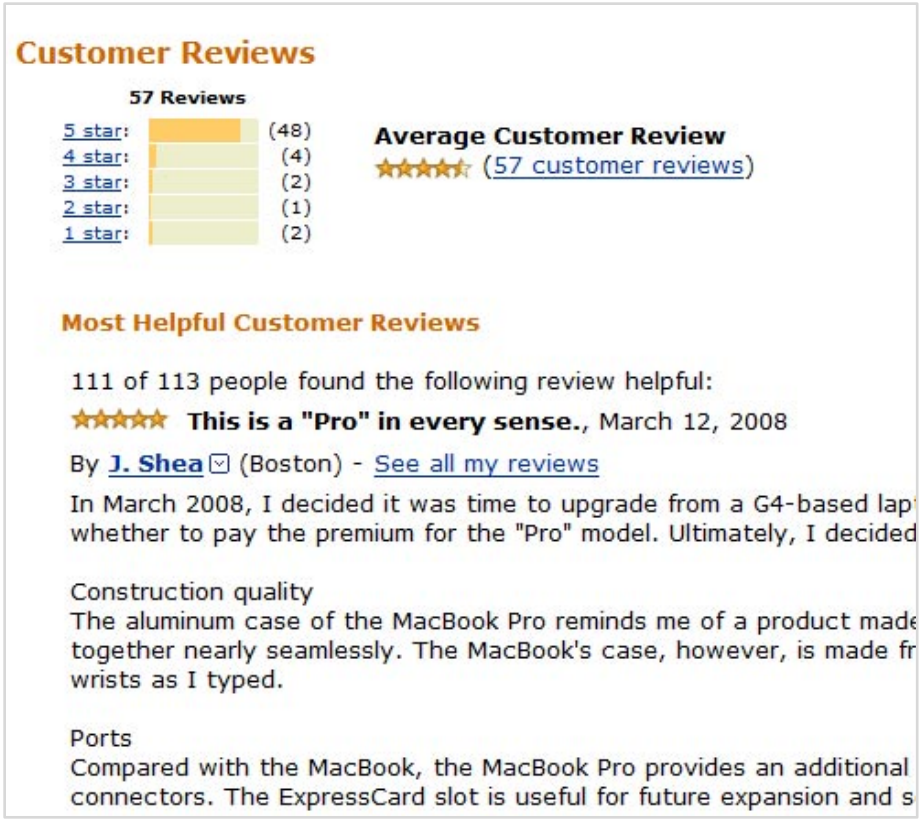
Crowd-Sourcing

…is when all or a significant portion of your content is provided by your user community

Leveraging community-generated content is extremely powerful

It Can Be Done Well…

- Amazon.com
- Internet Movie Database
- Wikipedia



Customer Reviews

57 Reviews

5 star:	(48)
4 star:	(4)
3 star:	(2)
2 star:	(1)
1 star:	(2)

Average Customer Review
(57 customer reviews)

Most Helpful Customer Reviews

111 of 113 people found the following review helpful:

This is a "Pro" in every sense., March 12, 2008

By J. Shea (Boston) - See all my reviews

In March 2008, I decided it was time to upgrade from a G4-based lap whether to pay the premium for the "Pro" model. Ultimately, I decided

Construction quality
The aluminum case of the MacBook Pro reminds me of a product made together nearly seamlessly. The MacBook's case, however, is made fr wrists as I typed.

Ports
Compared with the MacBook, the MacBook Pro provides an additional connectors. The ExpressCard slot is useful for future expansion and s

An Amazon Review

Can We Do More?

Yes

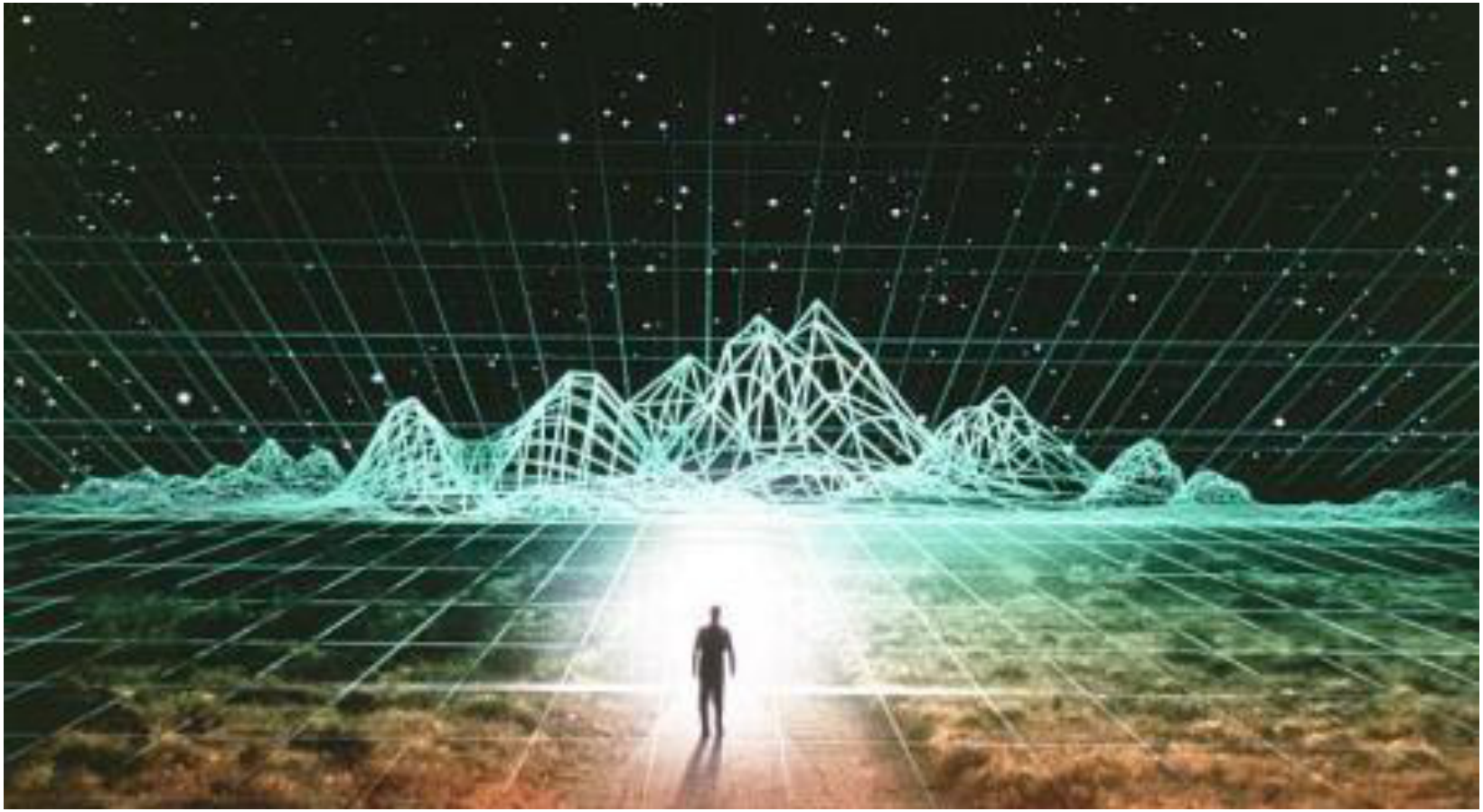
Because User Activity is Tracked

Usage Patterns & Statistics

- We can highlight popular Sightings / Indicators
- We can analyze viewing trends

Can We Do More?

Yes



Because We Know a Lot More About Our Users

About Our Users

We know who creates:

- …good/bad Sightings & Indicators
  - As rated by the community
- …good/bad comments
  - As rated by the community

We know who likes:

- …good/bad comments
  - As rated by the community

High Quality Users

- We can identify “High Quality Users”

Shouldn’t a user…

…who consistently likes good data elements

carry more weight

than someone who consistently does not?

The End Effect

- Identify the best analysis at any given time
  - Keeps content value high
  - Minimizes distractions
- Emphasize contributions of High Quality Users
  - 80% of value from 20% of users
  - Make contributing worth the effort

Supporting Features

- Should have user profiles
- Should be able to follow another user's activities
  - The Sightings / Indicators they have entered
  - The comments they have entered
  - Their Up votes
- Reputation
  - A user's "reputation" should matter to them…
  - It should be visible anywhere they're listed

Leveraging High Quality Users

Acknowledge activities that benefit community…

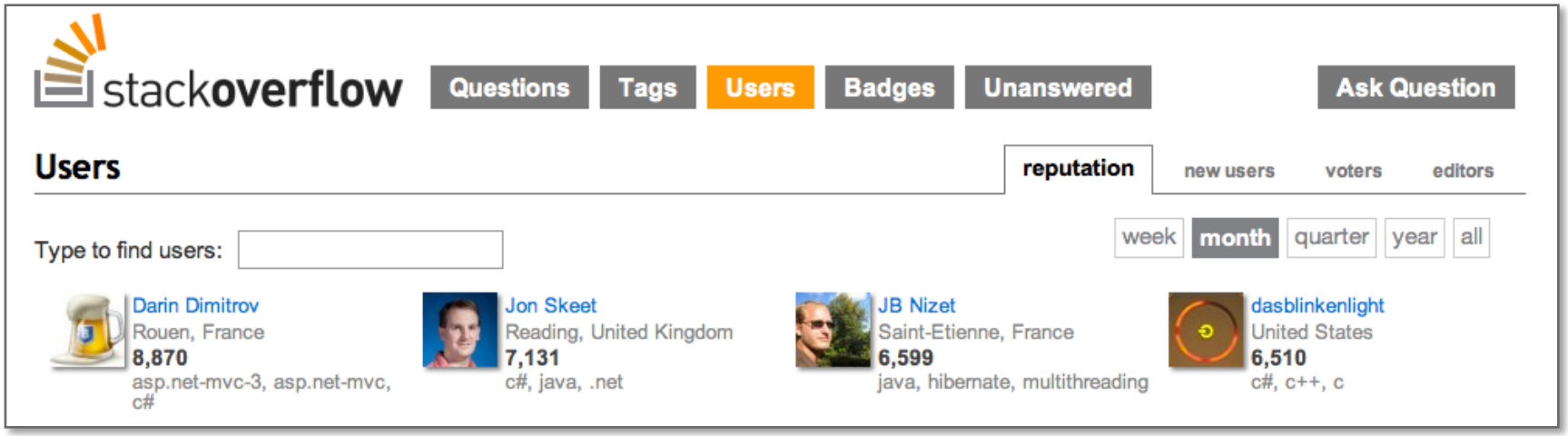
- Highlight "High Quality Users"
  - Visible display of their reputation
- Provide rewards for beneficial activities
  - Increased reputation (such as points)
  - Badges to highlight notable activities
  - Rank (as a potential credential)
- Encourage good activities

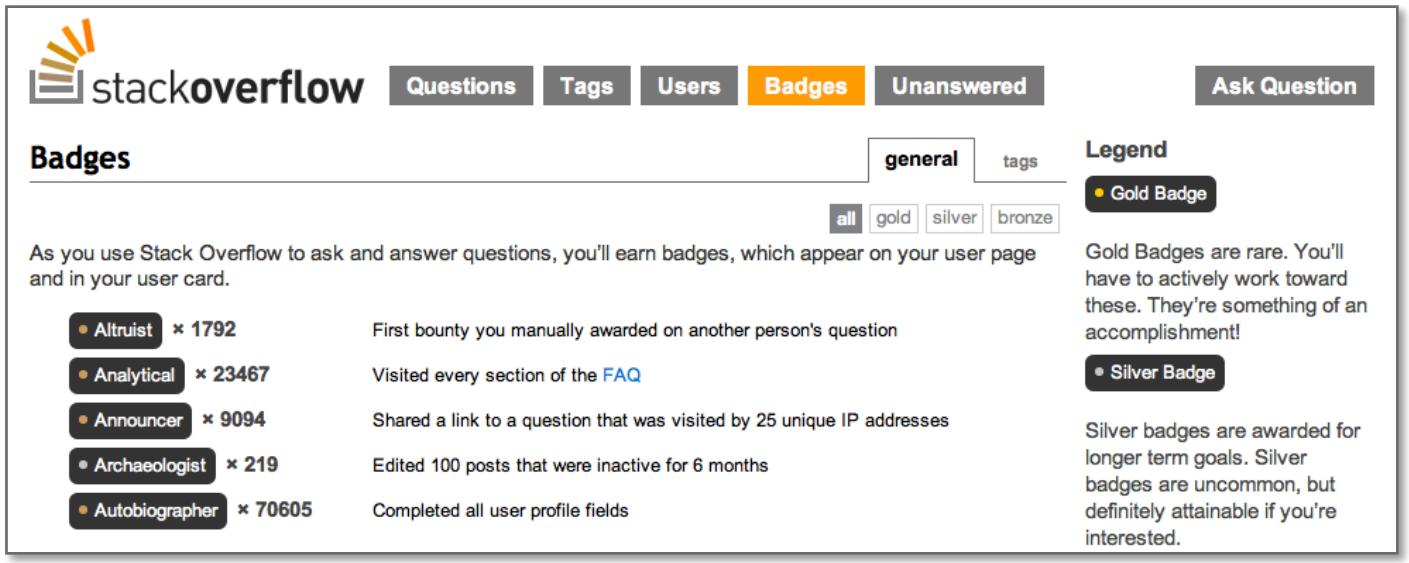
This Is “Reputation Ranking”

- Calculating user reputation based on community-related activities
- Leveraging reputation to highlight good content
- Using reputation to encourage a community to achieve the highest performance level

Pie In the Sky

Stack Overflow

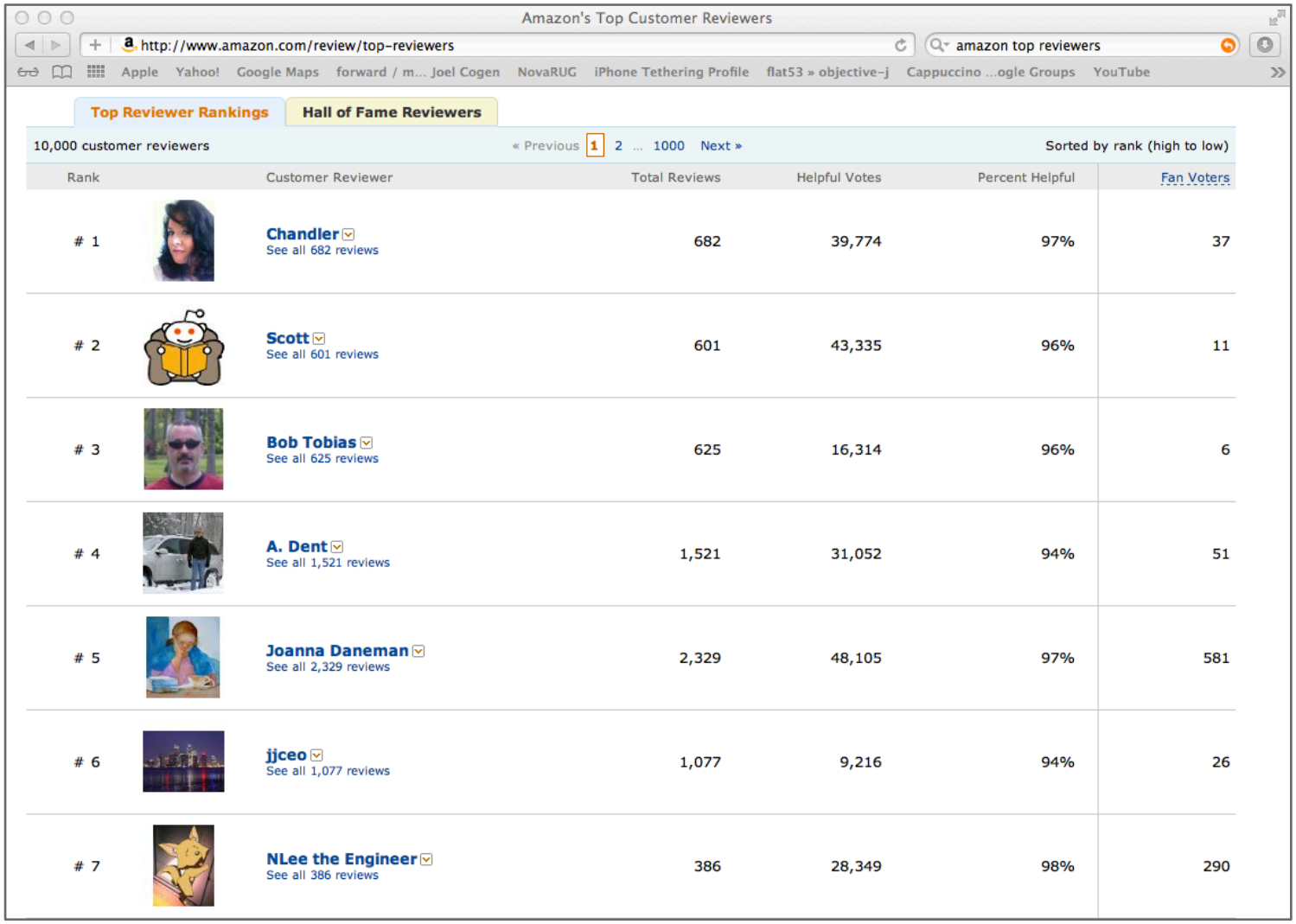




The Value of This Approach

- User-generated content
- User-rated content
- Well publicized reputation scores
- Rewards: User can earn extra privileges
- Badges: For ongoing encouragement

Amazon – Top Reviewers



Rank	Customer Reviewer	Total Reviews	Helpful Votes	Percent Helpful	Fan Voters
# 1	**Chandler** See all 682 reviews	682	39,774	97%	37
# 2	**Scott** See all 601 reviews	601	43,335	96%	11
# 3	**Bob Tobias** See all 625 reviews	625	16,314	96%	6
# 4	**A. Dent** See all 1,521 reviews	1,521	31,052	94%	51
# 5	**Joanna Daneman** See all 2,329 reviews	2,329	48,105	97%	581
# 6	**jjceo** See all 1,077 reviews	1,077	9,216	94%	26
# 7	**NLee the Engineer** See all 386 reviews	386	28,349	98%	290

But Wait! There's More!

A Recommendation Engine

- We know you like a particular Sighting
- Other people who like that Sighting ALSO like this other Sighting over here
- We can recommend things you might be interested in

Summary

The Indicators Sharing Platform uses:

- Crowd-Sourcing
  - To leverage community expertise
- Reputation Ranking
  - To highlight the most useful information
- Predictive Recommendations
  - To show you what you need to know
- Increased Information Dissemination
  - To help share what the community already knows

Part 3: Thoughts for the Future

Open Playing Field

New technologies bring new vulnerabilities that will be exploited by Bad Actors

- Increased use of Virtual Reality, e.g. – Second Life
- Augmented Reality
- New Devices – Smartphones, tablets, etc.

We need better ways to fight the Bad Actors

Collaboration Is Key

- Social Networking is about collaboration
  - It can be purely social like Facebook
  - But it can be harnessed for a real purpose
    - **Amazon:** High-quality product reviews
    - **Stack Overflow:** Real answers to real technical problems by real experts
    - **Indicators Sharing Platform:** Fighting the bad guys

Social Networking Techniques

…Can provide real benefits

- Crowd-Sourcing
  - To leverage community expertise
- Reputation Ranking
  - To highlight the most useful information
- Predictive Recommendations
  - To show you what you need to know
- Increased Information Dissemination
  - To help share what the community already knows

Social Networking Techniques

We've shown the benefits of…

- Crowd-Sourcing
- Reputation Ranking
- Predictive Recommendations
- Increased Information Dissemination

Combined, we have a Feedback Loop that can increase community effectiveness

Conclusion

The Bad Actors are getting more sophisticated.

Let's Harness the Cyber Security Community

And Hone It

Into an Even More Effective Weapon

Against Bad Actors

Questions

We can be contacted at:

David Keener
david.keener@gd-ais.com

David Roberts
david.a.roberts@gd-ais.com

Jonathan Quigg
Jonathan.quigg@gd-ais.com

Credits

1 - 5: General Dynamics Advanced Information Systems
6: Tombstone, AZ in 1881; http://www.rinodistefano.com/en/articles/tombstone.php
7: Matrix Wallpaper; ubiquitous.
8: Bio Pics; by permission of the presenters.
9: Twitter / Facebook; ubiquitous.
10: Empire State Building; Library of Congress Prints and Photographs Division
http://science.howstuffworks.com/engineering/structural/empire-state-building.htm
12: Louisville Slugger; ubiquitous product picture.
16: Security; http://icons.mysitemyway.com/free-clipart-icons/1/locked-padlock-icon-with-keyhole-id/75827/style-id/584/3d-glossy-blue-orbs-icons/business/
17: What Can I Do? Unknown source.
19: Envelope; http://icons.mysitemyway.com/free-clipart-icons/1/envelope-shaped-icon-variation-id/75766/style-id/584/3d-glossy-blue-orbs-icons/business/
20. Traffic Light Protocol; US-CERT; http://www.us-cert.gov/tlp/
21: Social Networking; http://prblog.typepad.com/strategic_public_relation/2007/06/top-10-reasons-.html
25: Couch Potato; http://www.flickr.com/photos/joebehr/4794268433/

Credits (2)

26: TV Remote; by Bradley P. Johnson.
http://www.flickr.com/photos/bradleypjohnson/5412154457/sizes/l/in/photostream/
27: Dog Watching TV; by maufdi.
http://www.flickr.com/photos/11335395@N06/3233723212/sizes/l/in/photostream/
29: Grain and chaff; From Wikipedia; http://en.wikipedia.org/wiki/Chaff
30: Stack Overflow Screenshot.
31: Relevancy; From the Sharpie Blog; http://blog.sharpie.com/2010/07/highlight-whats-right/
33: Checkmark; http://www.website-building-and-hosting.com/
35: Amazon.com Screen Shot.
40: The Edge; Publicity graphic for *The Thirteenth Floor* ;Tristar Pictures, 1999.
41: Knowledge; http://www.instructables.com/id/How-to-Train-Your-Brain-for-Free/
43: Wooden Thumb; http://icons.mysitemyway.com/
47: Pie in the Sky; http://newspaper.li/pie-in-the-sky/
48: Stack Overflow Screen Shots.
50: Top Reviewers; Amazon.com Screen Shot.
51: General Dynamics Advanced Information Systems