Advantages to Aggregation and Coordination

Notes for Karl Levitt & Friends

8 Feb 2002

Todd Heberlein

todd@NetSQ.com

530-758-4338

Outline

- Overview of process.
- Detecting subtle attacks.
- Pooling expertise for interpretation.
- Predicting attacks to prepare for attacks.
- Distinguishing between random acts of violence and targeted attacks.
- Interdicting fast moving attacks.

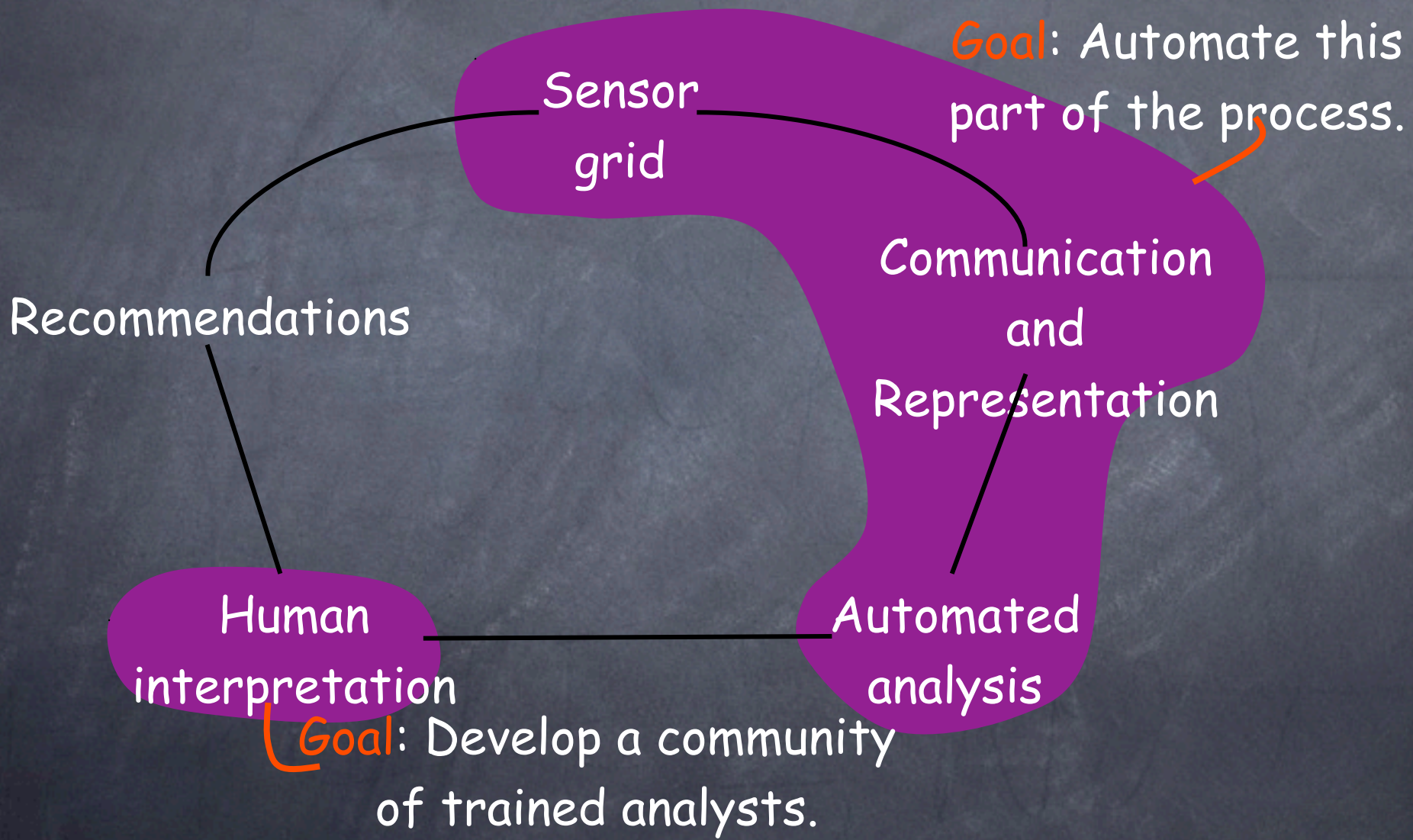
Surveillance

Surveillance is the *ongoing systematic* collection, collation, analysis and interpretation of data; and the dissemination of information to those who need to know in order that action may be taken.

Principles of Disease Surveillance
World Health Organization

http://www.who.int/emc/slideshows/Survintro/sld001.htm

The Process


Goal: Automate this part of the process.
Sensor grid
Communication and Representation
Recommendations
Human interpretation
Automated analysis
Goal: Develop a community of trained analysts.

Outline

- Overview of process.
- **Detecting subtle attacks.**
- Pooling expertise for interpretation.
- Predicting attacks to prepare for attacks.
- Distinguishing between random acts of violence and targeted attacks.
- Interdicting fast moving attacks.

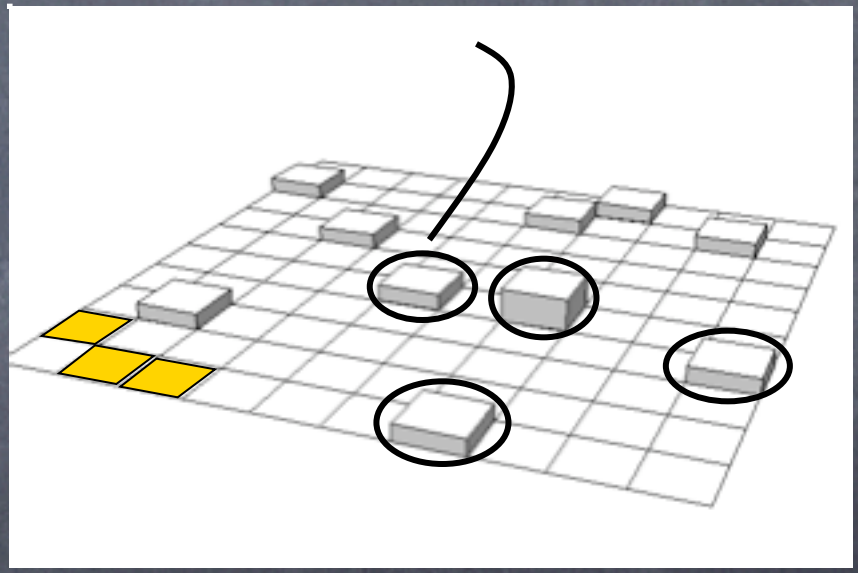
Intrusion Detection Paradox

- Most sensors today are only useful for detecting already known attacks with existing solutions.
  - Wouldn't it be better to simply apply the solution?
- Would the vast majority of administrators know what to do if a sensor reports a previously unknown attack against a previously unknown vulnerability?
  - It is hard enough to get people to use "Live Update"
  - Is there a commercial market for such sensors?

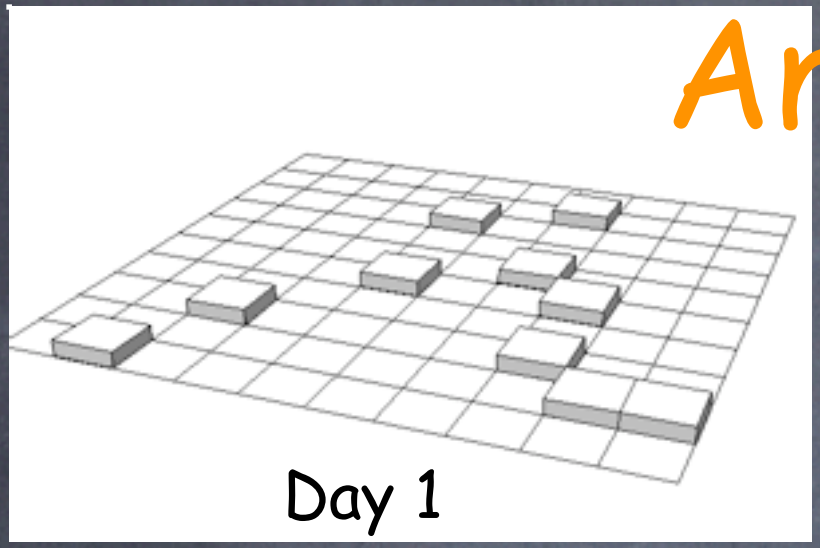
Interface of Unusual Events

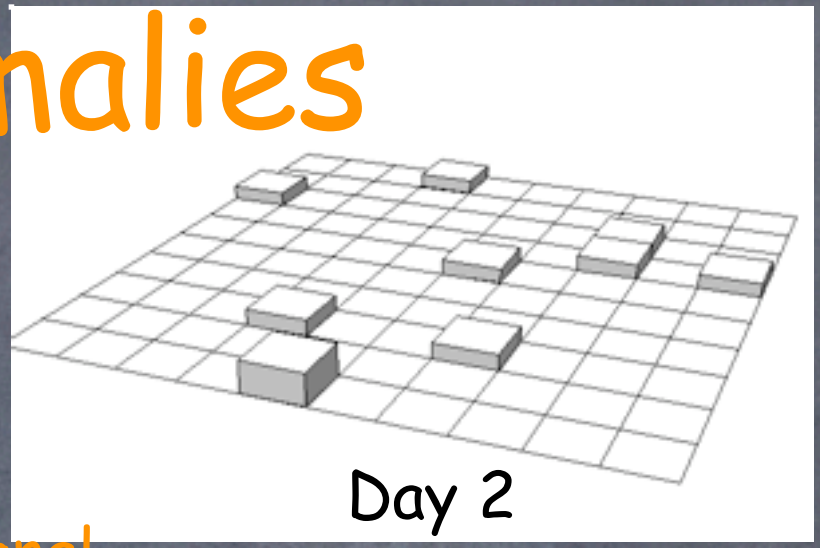
- Each cell represents a different report type.
- One "event" was reported for each of these types.
- Two "events" reported for this type.
- Which report is associated with attack?

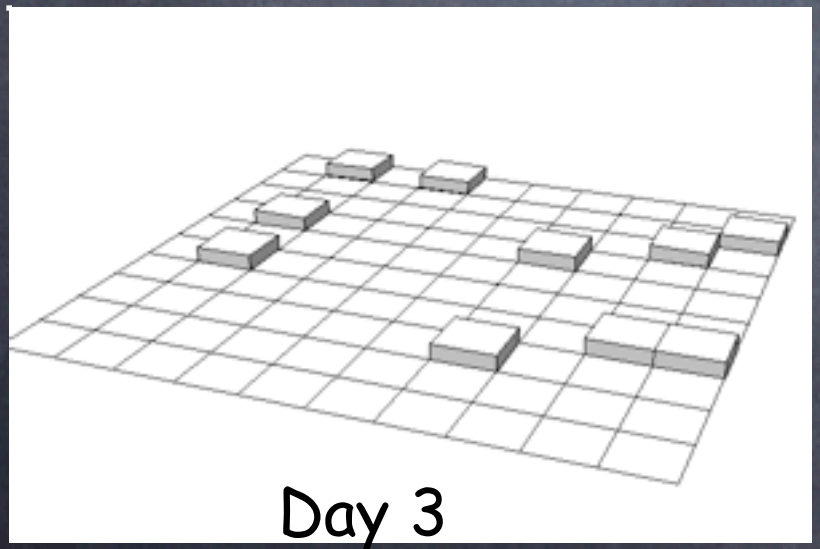
The only anomaly generated by the attack



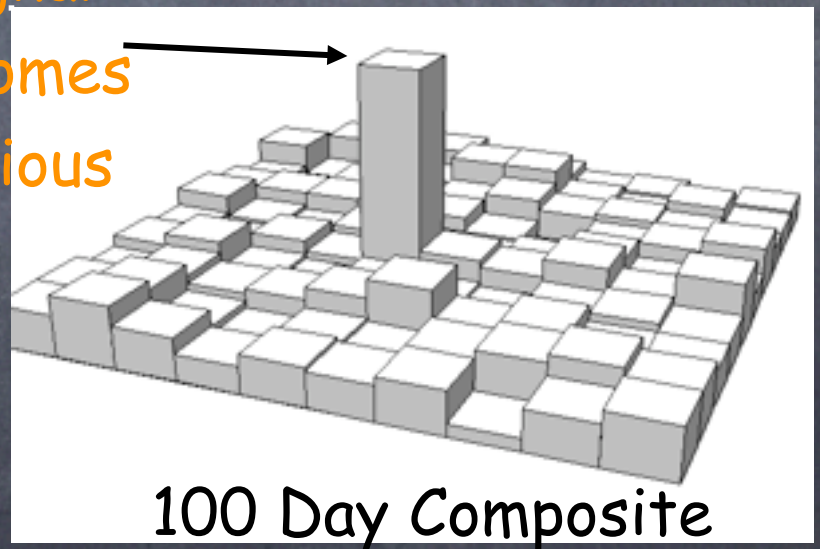
Aggregation of Anomalies



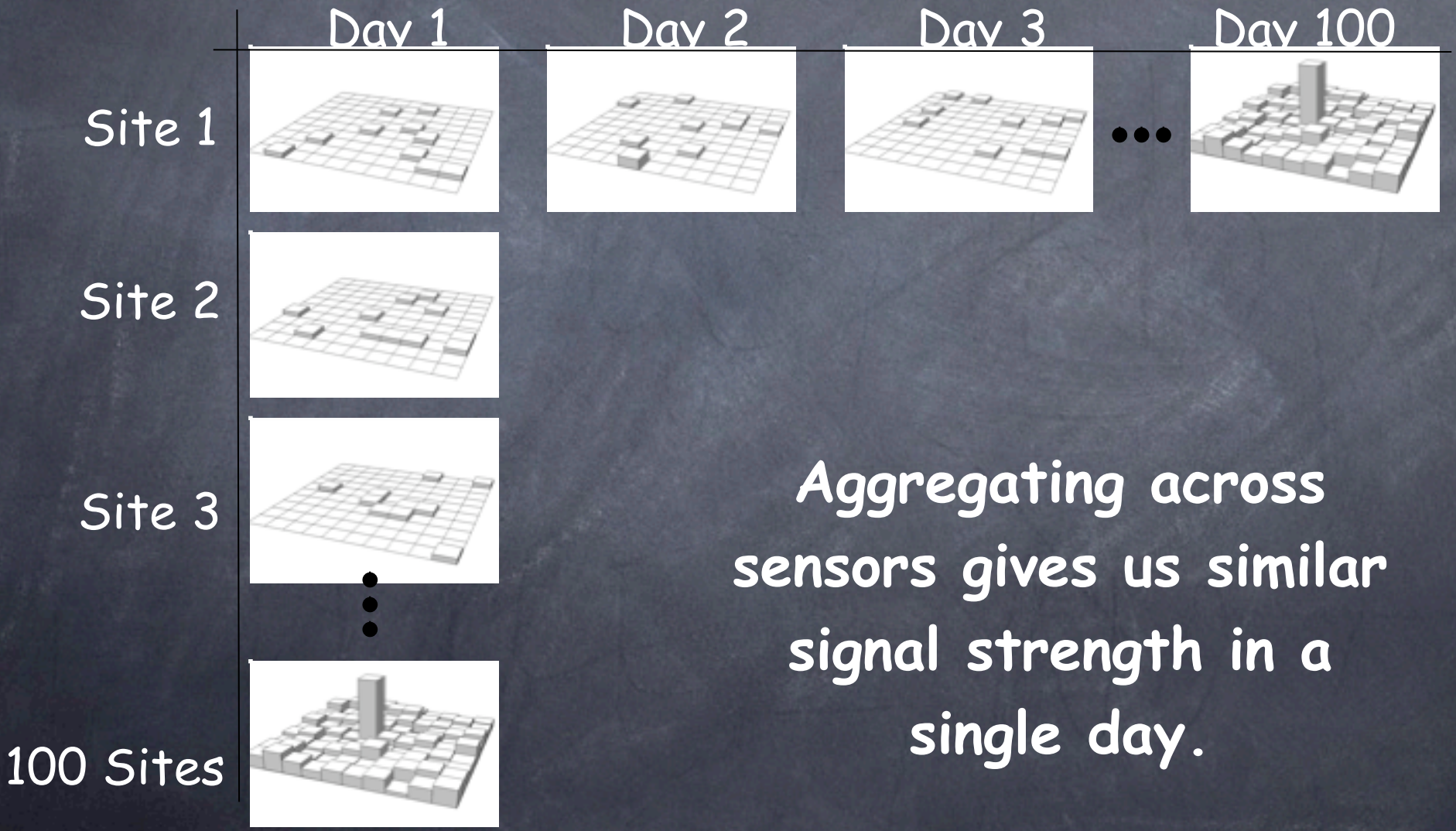




Signal becomes obvious



Aggregation Across Sites



Aggregating across sensors gives us similar signal strength in a single day.

Outline

- Overview of process.
- Detecting subtle attacks.
- **Pooling expertise for interpretation.**
- Predicting attacks to prepare for attacks.
- Distinguishing between random acts of violence and targeted attacks.
- Interdicting fast moving attacks.

Human Interpretation

- Even today's sensors are capable of detecting new and subtle threats, but few can understand what is being detected.
- Structures found within large amounts of distributed data will need to be interpreted.
- Too many operating systems, applications, protocols, and programming languages.
  - No single organization can field the expertise to diagnose all potential new threats.

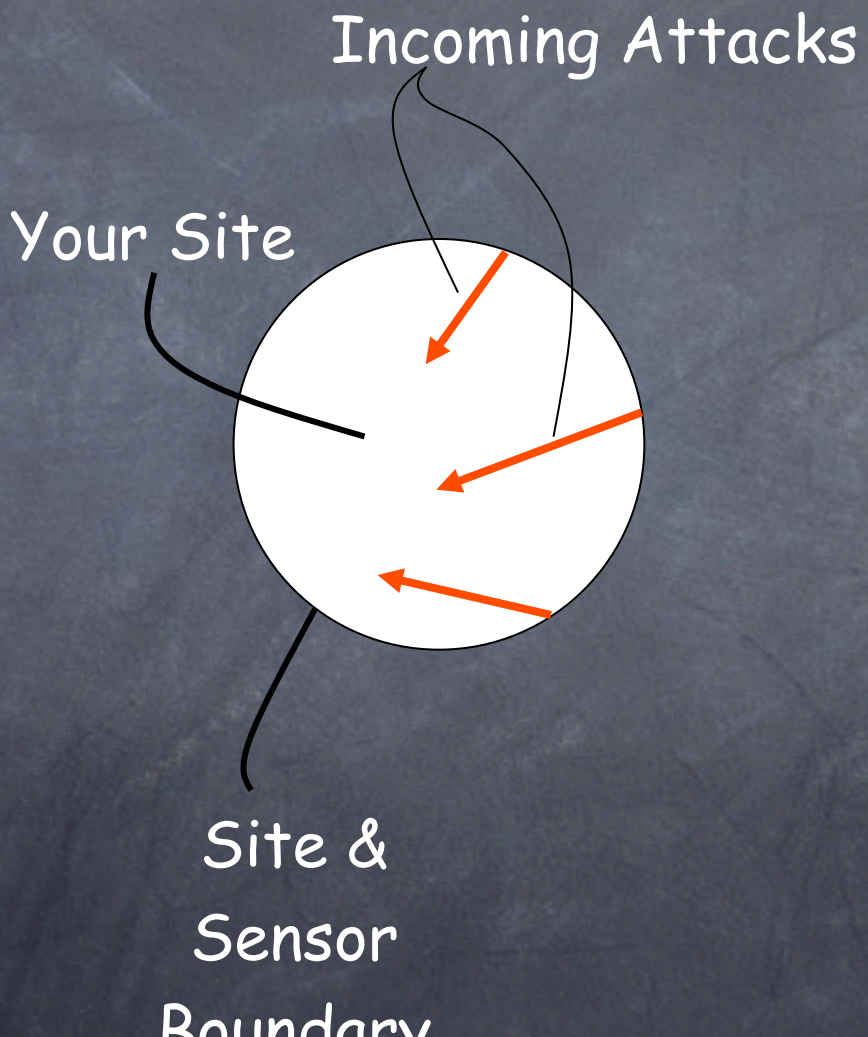
Outline

- Overview of process.
- Detecting subtle attacks.
- Pooling expertise for interpretation.
- **Predicting attacks to prepare for attacks.**
- Distinguishing between random acts of violence and targeted attacks.
- Interdicting fast moving attacks.

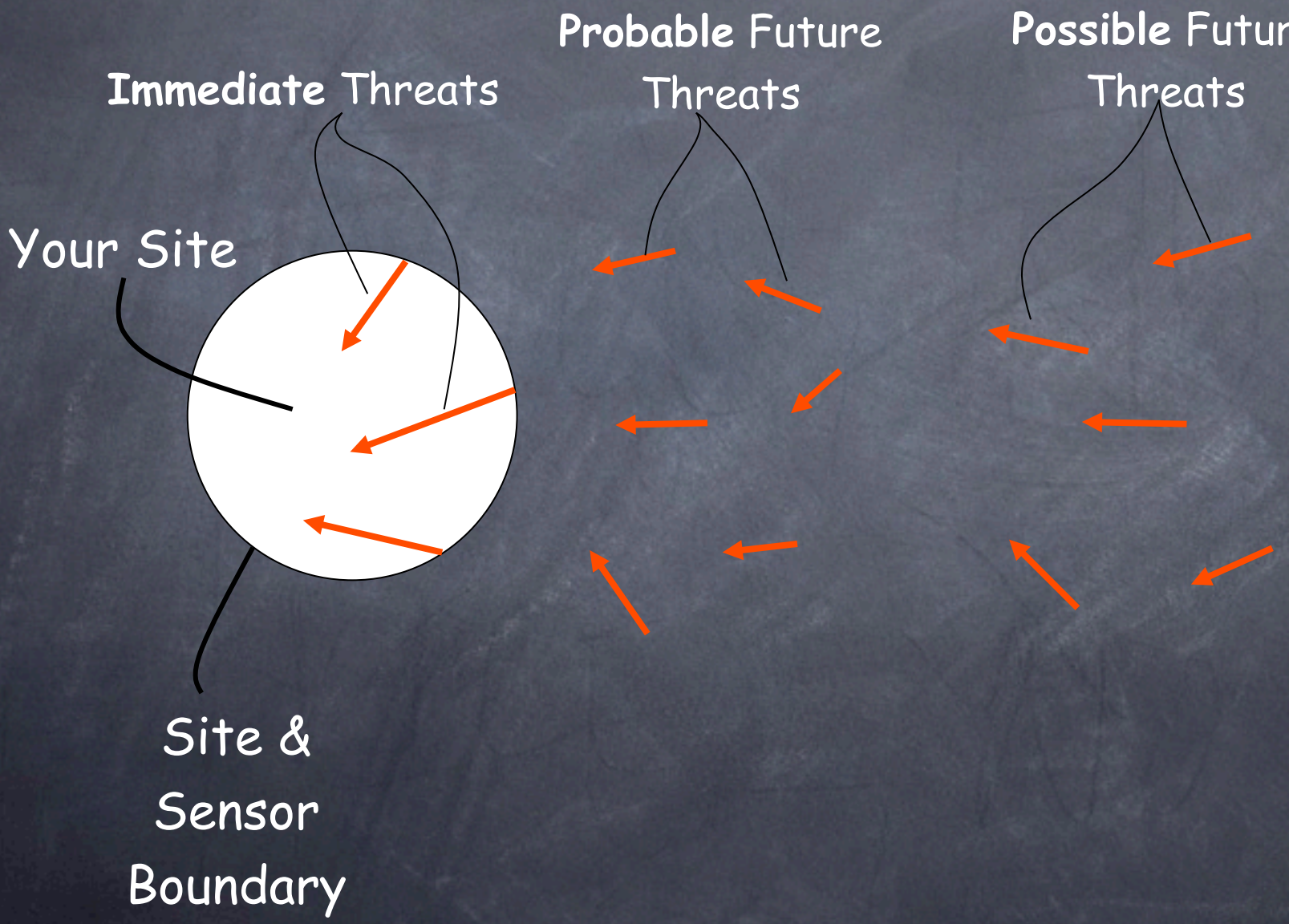
Detection to Prediction

- Use sensors to predict the attacks before they occur
- Requires shared, correlated reporting
- Amazon model
  - Amazon has millions of books, but they have a very limited opportunity to present to you books they think you will buy.
  - There are hundreds or thousands of vulnerabilities at any site, but a system administrator has time to fix a small number.

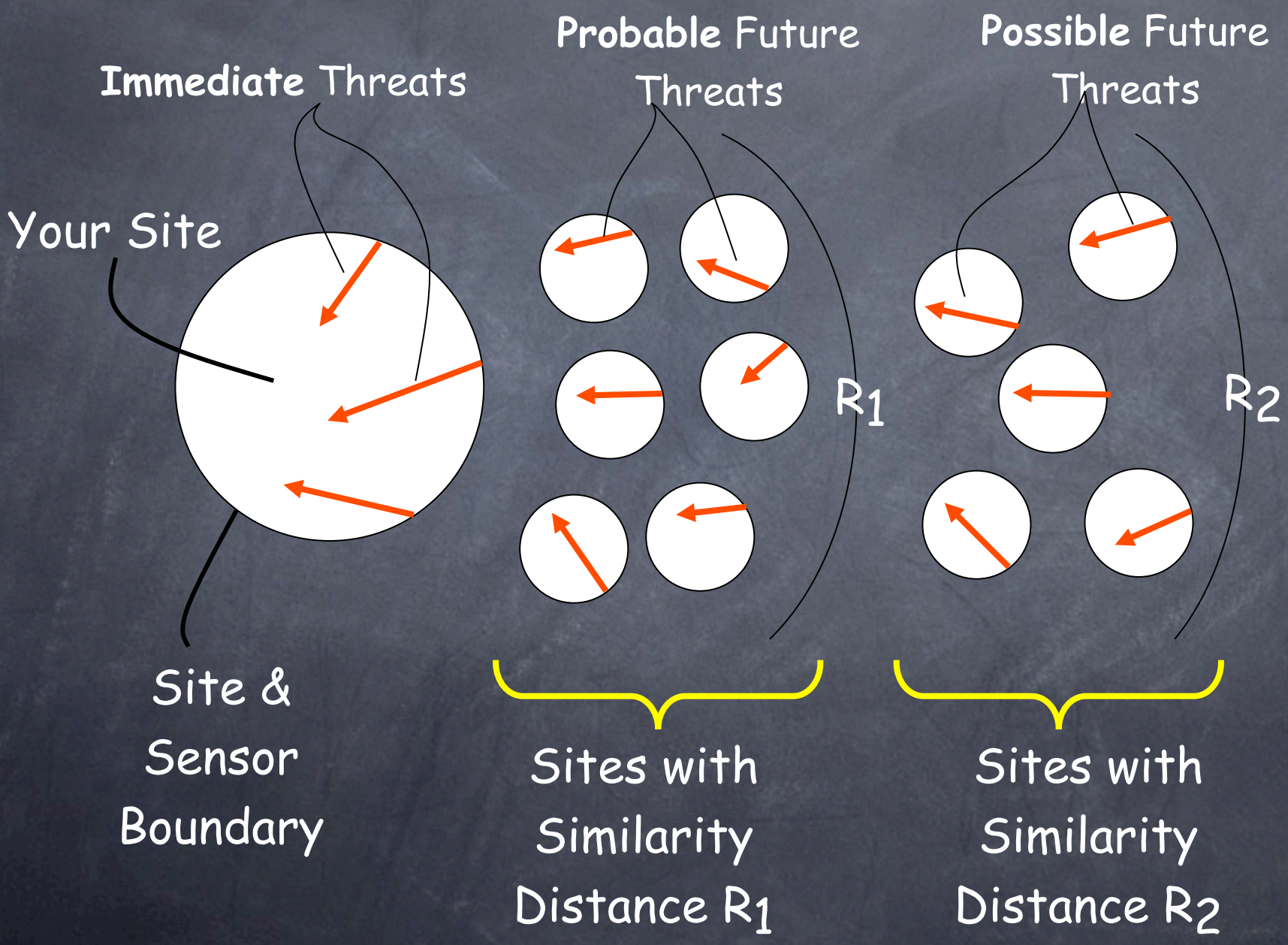
Today's Myopic Sensor View



Over the Horizon Threat Detection



Nearest Neighbor Sensor Coordination



Outline

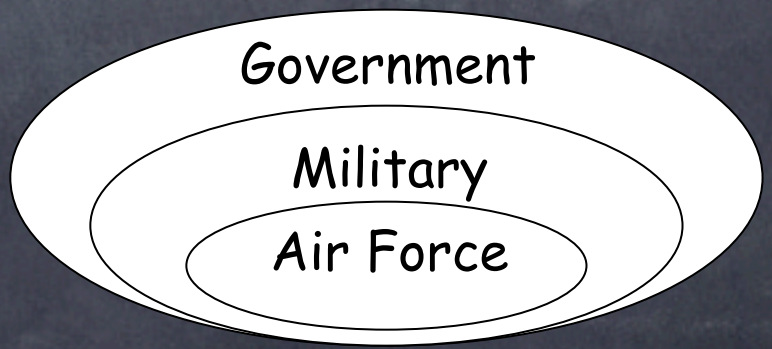
- Overview of process.
- Detecting subtle attacks.
- Pooling expertise for interpretation.
- Predicting attacks to prepare for attacks.
- **Distinguishing between random acts of violence and targeted attacks.**
- Interdicting fast moving attacks.

Amazon Techniques

- Top sellers
- Movers and Shakers
- Top sellers unique to your defined group
- Books purchased by those who look the most like you

Amazon Purchase Circles

- Identifies top sellers unique to defined groups.
- Groups are defined a priori
- Our model:
  - may indicate an attack targeted at a specific group (e.g., Air Force or power grid)



Bestsellers for U.S. Air Force

1. Harry Potter and the Goblet of Fire
2. Harry Potter and the Chamber of Secrets
3. Harry Potter and the Sorcerer's Stone
4. Harry Potter and the Prisoner of Azkaban

Activity unique to Air Force, and perhaps most important to the Air Force, is lost in the noise.

Unique to U.S. Air Force

1 Air Power: A Centennial Appraisal

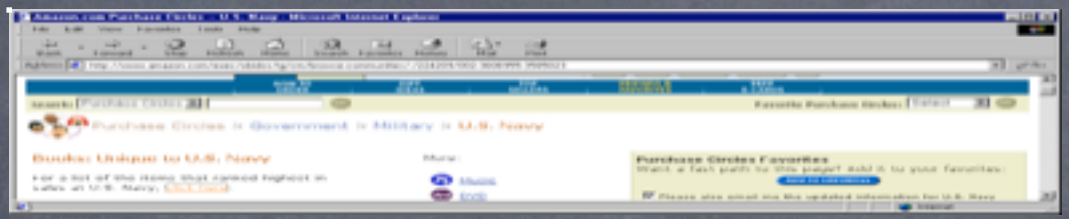
2 They Also Flew: The Enlisted Pilot Legacy, 1912-1942

3 Victor Padrini: A Novel of the United States Air Force Academy

4 The Limits of Air Power: The American Bombing of North Vietnam

These books are important to people in the Air Force. What attacks might be unique to the Air Force, and should we pay closer attention to them?

Unique to U.S. Navy



1. Jane's Fighting Ships 1999-2000
2. Jane's Fighting Ships 2000-2001
3. The Naval Institute Guide to Naval Writing
4. Naval Operations Analysis

Outline

- Overview of process.
- Detecting subtle attacks.
- Pooling expertise for interpretation.
- Predicting attacks to prepare for attacks.
- Distinguishing between random acts of violence and targeted attacks.
- **Interdicting fast moving attacks.**

Fast Attacks

- Example Fast Attacks
  - Morris Worm, Melissa, ILOVEYOU, Code Red
- Common Features
  - Reached ~100% penetration before countermeasures ready.
  - Mostly benign "malicious" code.
  - Coders worked alone, on their spare time, were not intending to cause great harm

Fast Attacks Continued

- How fast can they get?
  - Warhol: complete penetration < hour.
  - Flash: complete penetration < few minutes.
  - Designs available on the web.
- Potential Damage
  - Change passwords on hardware (BIOS, printers).
  - Damage disks.
  - Smoke monitors.
  - Damage, release data.

Summary

- Overview of process.
  - Model after CDC.
- Advantages
  - Detecting subtle attacks.
  - Pooling expertise for interpretation.
  - Predicting attacks to prepare for attacks.
  - Distinguishing between random acts of violence and targeted attacks.
  - Interdicting fast moving attacks.