

Detecting Insider Threat Behavior

Greg Stephens

703-883-3242 •
gstephens@mitre.org

MSR/FY2004: \$570K / FY2005: \$580K / FY2006: \$520K



MITRE
Technology
Program

Problem

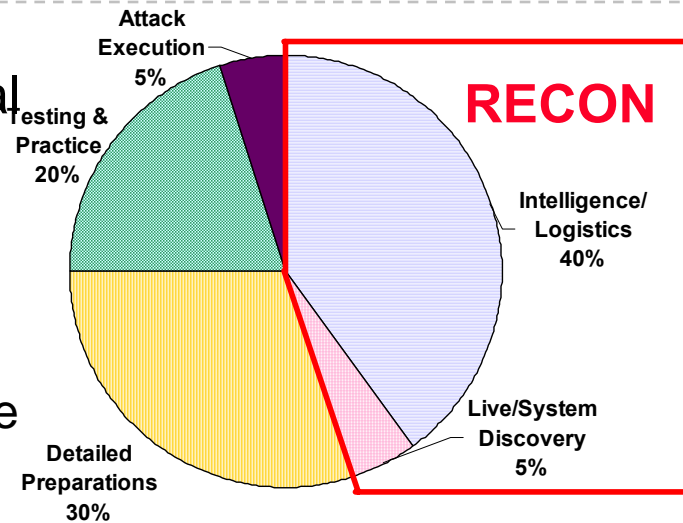
- **Trusted insiders committing espionage have caused tremendous damage to U.S. national security**
- **Sensitive U.S. information is vulnerable to insider misuse**
 - **More information to protect than ever**
 - **Need to know impossible to enforce**
 - **Post 9/11 drive to share across boundaries**
- **Effective information misuse detection mechanisms do not exist**

Background

■ Observation #1

Reconnaissance is an essential step for the malicious insider

- National Intelligence Council Cyber Threat Estimate
- Red team activity analysis
- MITRE operational experience



2000 Insider Threat Workshop Proceedings

■ Observation #2

Need context to differentiate reconnaissance from legitimate information use

- Organizational (formal, relatively static)
 - e.g. organizational structure, user directory information
- Behavioral (informal, relatively dynamic)
 - e.g. communities of interest

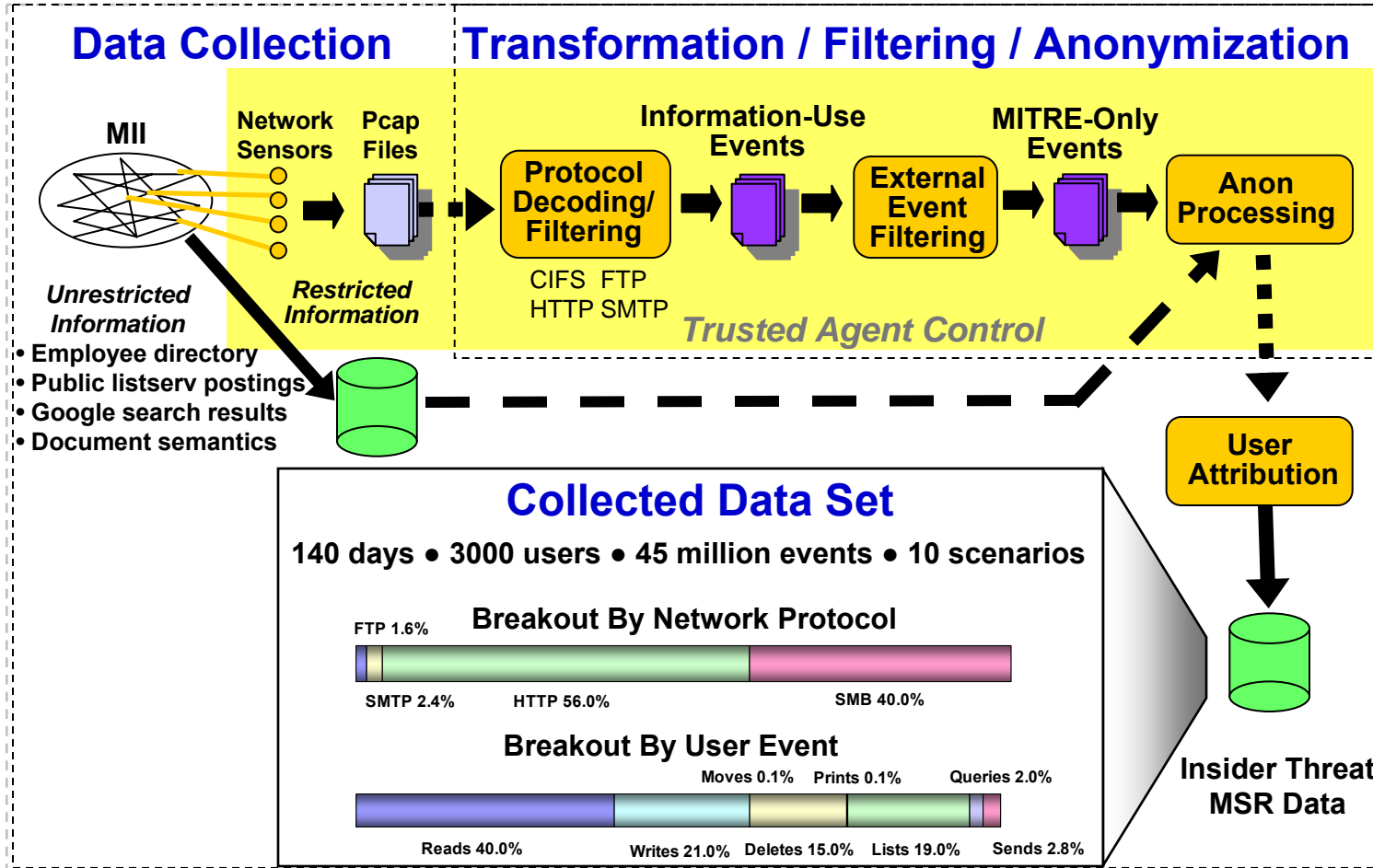
Objective

- **Develop sensors to collect data streams closely tied to information use; attribute to users**
- **Build information and user context from available sources**
- **Develop context-sensitive rules that identify insider reconnaissance**

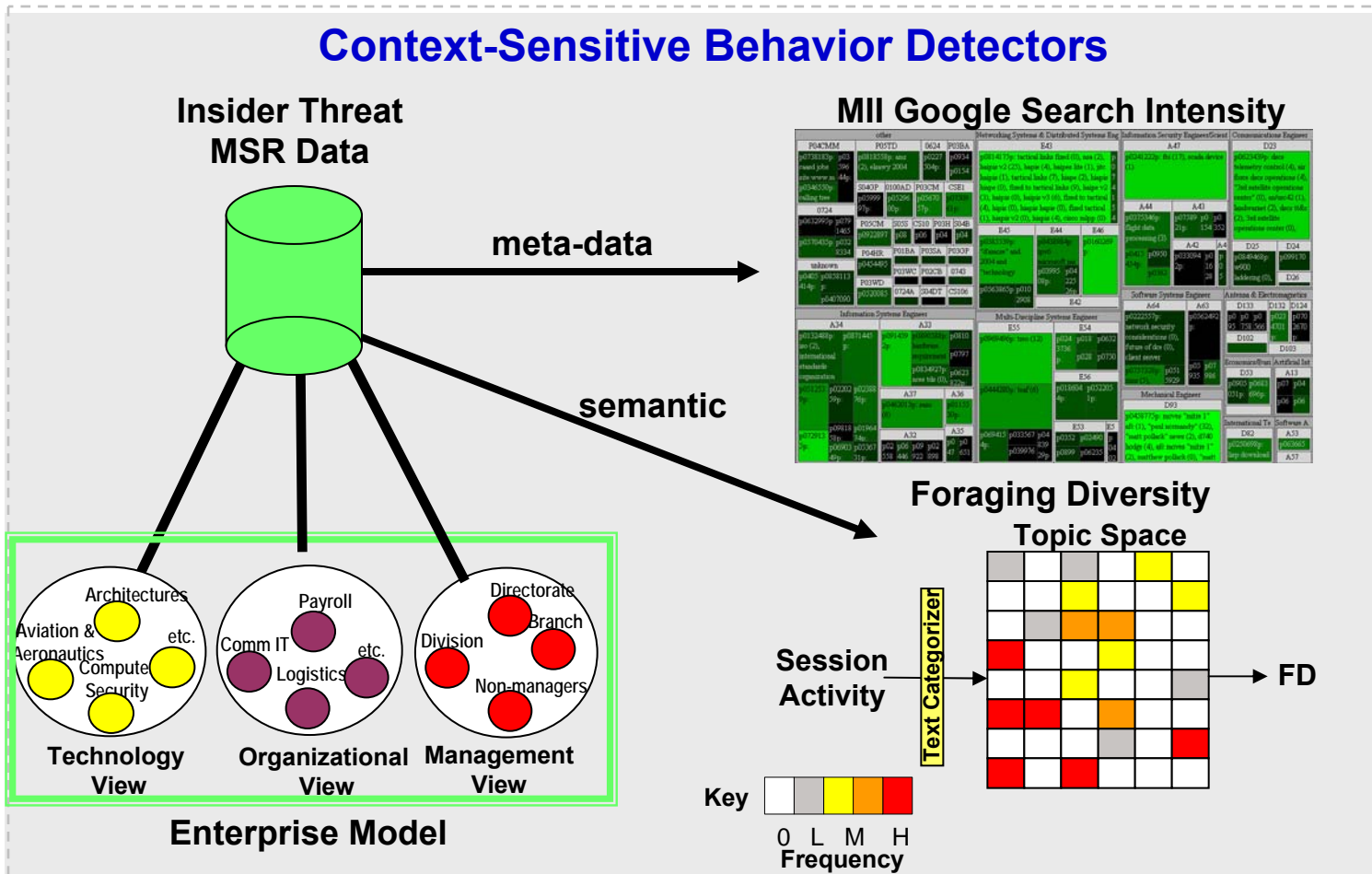
Activities

- **Developed information use sensors**
- **Executed red-team scenarios**
- **Collected, processed, and anonymized testing data set**
- **Developed user attribution algorithms**
- **Developed reconnaissance detectors**
- **Applied detectors to data set**

Highlight



Demonstration



Impacts

- **Demonstrate that insiders can be detected BEFORE they damage U.S. national security**
- **Transition technology to MITRE sponsor base**
- **Develop sharable reference data set for insider threat research community**
- **Enable increased information sharing**
 - **Share but monitor for abuse**

Future Plans

Develop Indicator-Based Threat Scoring System

