

# Computer Crime

## A Data Centric View

Raffael Marty, GCIA, CISSP  
Chief Security Strategist @ Splunk>

CSI 2007 - San Francisco

# Agenda

- Shifted crime landscape
- Have you shifted?
- Watch it
- IT Search

# Shifted crime landscape

- Crimes are moving up the stack
  - Web 2.0 attacks
  - IM / messaging attacks
- Targeted attacks
- Insider crime
  - fraud
  - sabotage / abuse
  - information leaks
- Everyone can be a victim



# Have you shifted?

- Are you prepared?
- Are you monitoring?
  - Do you know what is happening right now?
- Are you monitoring enough?
  - Monitor up the stack
  - Monitoring applications

Eat Everything



Go Wicked Fast



Questions are not known in advance!  
Have the data when you need it!

# Watch it!

- Centralized data collection
- *All* the data
  - application logs
  - network equipment
  - configuration files
  - real-time performance measures
- More and other data sources than for the traditional security use-cases



# IT Search

1. Universal Real Time Indexing
2. Ad-hoc Search & Navigation
3. Interactive Alerting & Reporting
4. Knowledge Capture & Sharing
5. Scalable Deployment
6. High Performance Architecture
7. Secure Data Management





# Thank You

[www.splunk.com](http://www.splunk.com)

[raffael.marty@splunk.com](mailto:raffael.marty@splunk.com)