Open Sourced Intelligence and Industrial Control Systems

LIVE DEMO v1.1

Presenter

- Joe Cummins, PCIP
  - Canadian Information Security practitioner as well as President and Principal Consultant of Red Tiger Security - Canada, which provides Threat and Vulnerability assessments to its growing client base both Nationally and Internationally.
    - SME in the areas of Critical Infrastructure and Federal Readiness;
    - Engaged as both speaker and instructor for all levels of public and private departments.

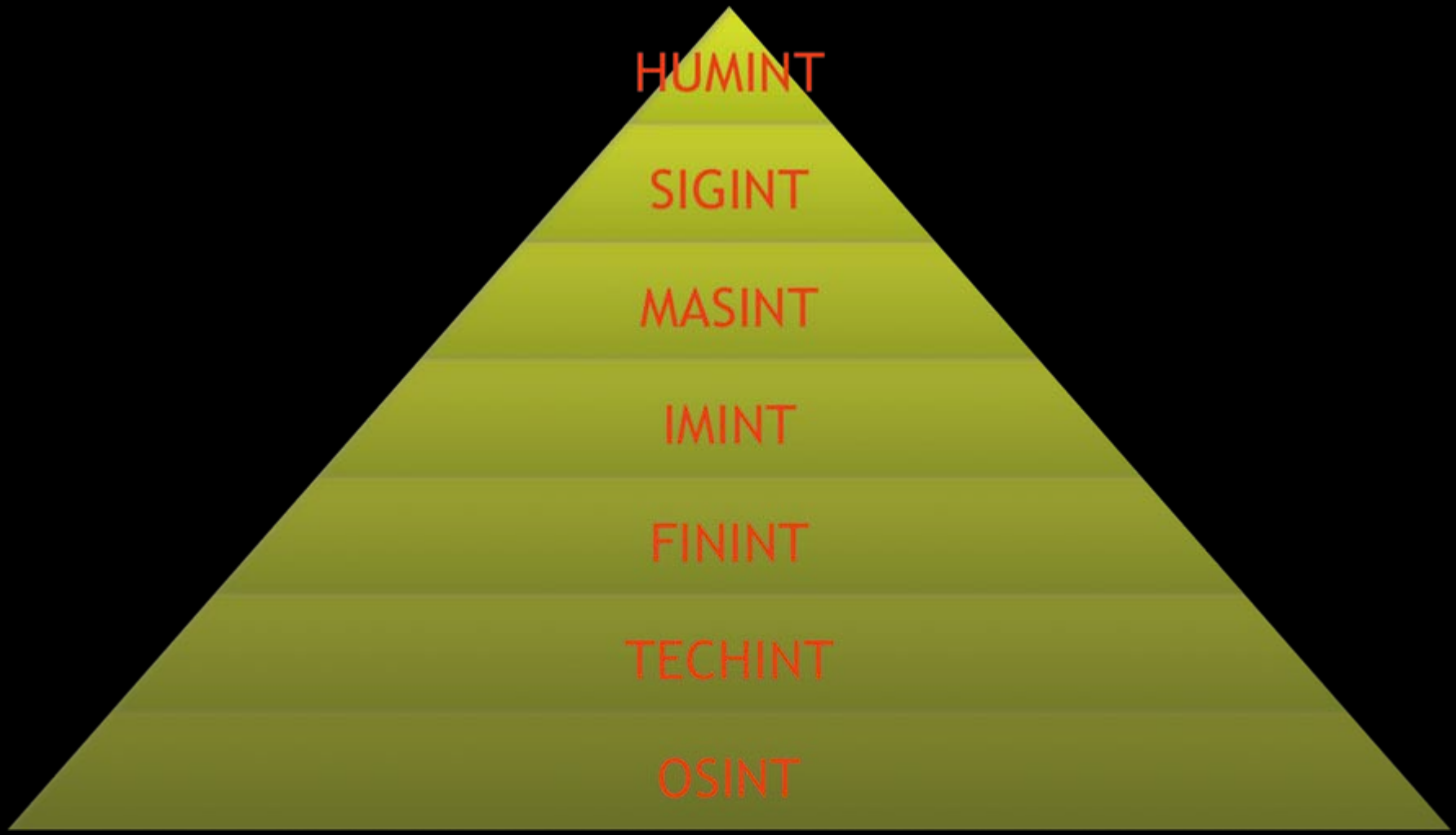
Agenda

- Levels of Intelligence
- Intelligence Pyramid
- Types of Linkages
  - Tangible
  - Intangible
- Sources
- Methodology
- Demonstration

Intelligence Pyramid

HUMINT	Human intelligence
INTEL	Intelligence
COINTEL	Counterintelligence
SIGINT	Signals intelligence
COMINT	Communications
ELINT	Electronic
FISINT	Foreign Instrumentation
MASINT	Measurement & signals
FININT	Financial Intelligence
IMINT	Imagery
TECHNINT	Technical information
OSINT	Open source intelligence

Intelligence Pyramid – Cont'd



Information Leakage

- Pieces of the puzzle
  - Small information
  - Lots of Frequency
  - Common linkage

- Footprinting
  - Digital breadcrumbs left behind for someone with enough time and skill to draw together a abstract image of the Internal Process.
  - Any data or information that is sensitive or potentially critical in nature

Threat to self – Threat to others

- Data that is posted
- Information posted about us
  - Spread across multiple sites
  - Increases the vulnerability Personally and professionally
- Investigative skill + malicious mindset

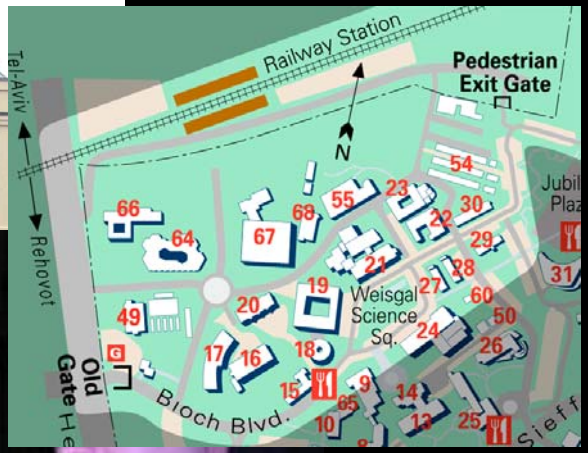
Tangible

- Emails
  - Naming convention
    - First.Last@work.com?
- Names
  - Additional Employees
  - Past Employees
- Phone Numbers
  - Direct Lines
  - PBX, VOIP
- Sever Addresses
  - Location
  - Lookup

Intangible

- Vague
- Non-Specific
- Usually incorporates multiple entities or layers of sources
- Conceptual relationships or bonds

Photos



ASC
ACME SPECIALTY CHEMICAL
The chemicals you need ...when you need them.

Phrases

- Sector specific
  - Language used within the community
  - Common terms
  - Acronyms
- Culture specific
  - Words
  - Language
  - Colloquial
- Location specific

Infrastructure Assets

- SMTP
  - Primary, Secondary
  - Useful email addresses
- WEB
  - Main site
  - Additional sites
- DNS
  - Internal / External
- Observe:
  - Naming conventions
  - Common themes
  - Common elements
  - Structures

Employment Sites

- Workopolis:
  - Employers:
    - Posting openings
- Monster.ca
  - Employers:
    - Posting openings
- Linkedin
  - Professional Networking Site
- Kompass
  - Online Business directory
  - French afil.
- Jigsaw:
  - Online business directory
  - Company Wiki

Canada411 – Information Lookup

- Personal Information
  - Addresses
  - Maps
  - Telephone Numbers
  - Postal / Zip Codes

- Reverse Lookup
  - For use in conjunction with other tools
  - Maltego

Social Websites

Networking

- Myspace
  - Social Networking
  - Pictures
  - Posting
- Facebook
  - Social Networking
  - Pictures
  - posting

Mail Based

- Live.Spaces.com
  - Social Networking
  - Pictures
  - posting
- Yahoo.com
  - Social Networking
  - Pictures
  - posting

New Media

- Podcasts
  - Economist
    - Direct insight into:
      - Cultures
      - Cities
      - Elections
      - Local Politics
      - Opinions
    - Weekly Synopsis
    - Interviews
    - State of the Nation Updates
    - Financial Spin
- RSS Feeds
  - Direct updates
  - Insider information
    - Opinions on Direction
  - Leading edge
    - Foreign Affairs
    - Macleans
- Mail Groups:
  - Universities
  - PHD students
  - Technical Groups

Method of Development

- Gathering
  - Discovering new and unique items or entities
  - Specific subsets
    - queried,
    - examined, and
    - Broken
- Gain
  - understanding of what is being represented
  - what findings are being made.
  - more insight into the
    - business operations or
    - enterprise systems.
- Synthesis
  - relationships between the various entities
  - gathering that has taken place for those specific discoveries.
    - Identification of relationships
    - Linkages that exist
    - Common Denominators
    - Extraction of specific information
- Pivot
  - Based on knowledge to date
  - Further queries
  - Extrapolation on known information or data

What does this mean to the Industry

- Concepts:
  - Insider information
  - Competitors advantage
  - Footprinting
  - Social Engineering
  - Physical

Demonstration

- Mock Assessment

Acme Specialty Chemicals