Cyber Intelligence: Concrete Analysis in a Fluid World

Coleman Kane
Coleman.Kane@ge.com
kaneca@mail.uc.edu
@colemankane
https://github.com/ckane

July 25 2015

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

/me

- Security Operations Technical Leader for GE Aviation
- Ph. D. candidate, Computer Science Engineering
  Cyber Operations track, University of Cincinnati
- B.S. Computer Engineering, University of Cincinnati
- CRITs project contributor
- FreeBSD community member & contributor since 2001
- 5 years experience in IT Security, 10 years in CS and IT
- Cincinnati native
- Running (because I like cake)
- 5 year old daughter
- Coffee aficionado
- Fancies cats

Introduction & Terminology

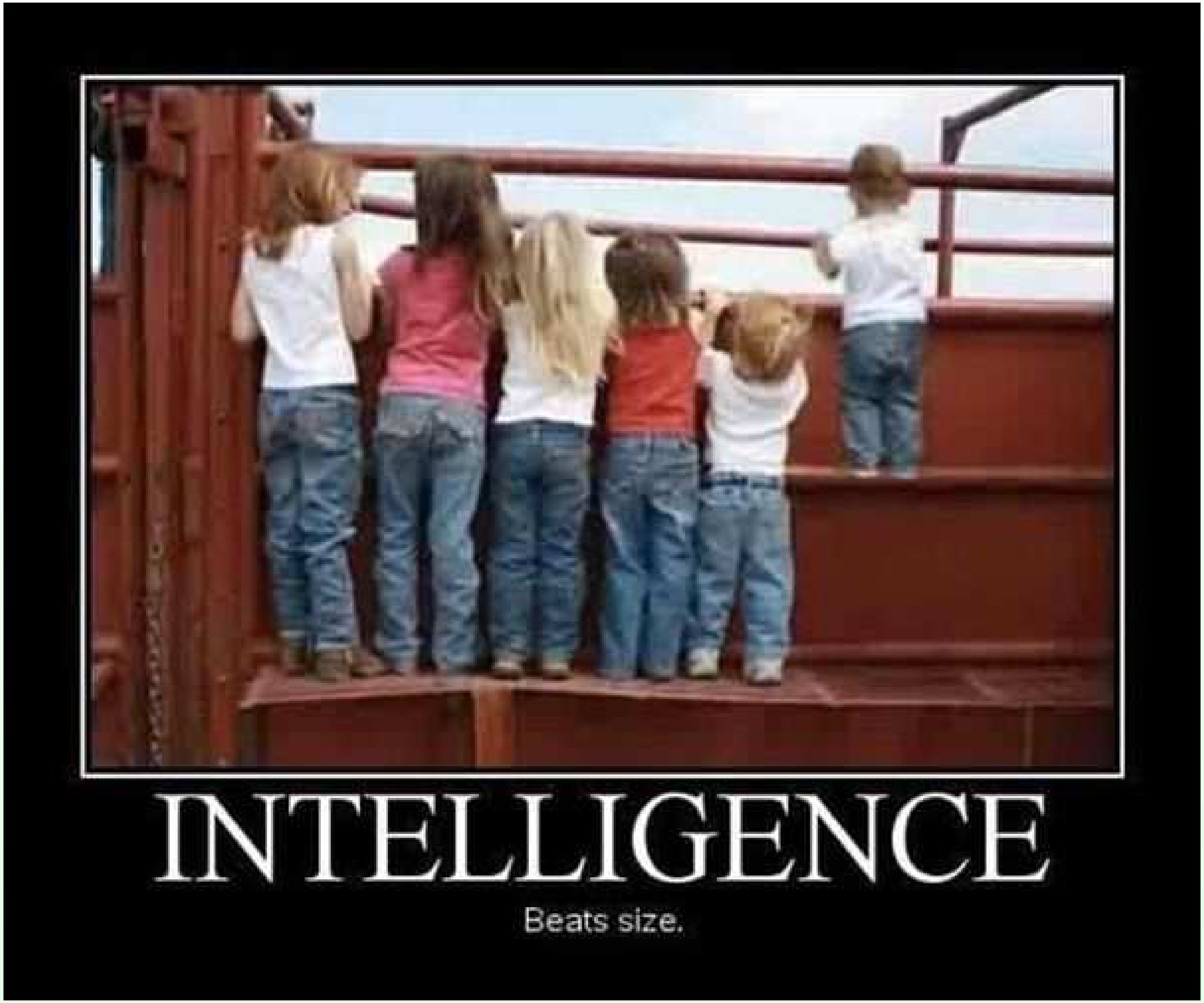
Threat Landscape The elements typically **outside of your control** that impact your security posture. This is where your threat actors, geopolitical policies, third-party postures, and similar factors exist

Attack Surface The elements **within your control/influence** impacting your security posture. Includes: Network design, user behavior, site geographies, security tools, etc. Considered frequently to be what you're defending against the **Threat Landscape**

Cyber Intelligence Knowledge of your threat landscape & attack surface. This can be in the form of structured/unstructured documentation, threat databases, tribal knowledge, situational awareness, and other formats

Introduction

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks



Certainty

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

Example of "certainty":

"*You don't get to operate in the world you want, you have to operate in the world you get.*" – Abraham Lincoln

Certainty

Example of "certainty":

"*You don’t get to operate in the world you want, you have to operate in the world you get.*" – Abraham Lincoln [*citation needed*]

Certainty

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

Example of "certainty":
"*You don't get to operate in the world you want, you have to operate in the world you get.*" – Abraham Lincoln [*citation needed*]

Environment is constantly in flux:

- **Attack Surface** - Lockheed Martin buying Sikorsky from UTC:

  `http://www.wsj.com/articles/lockheed-agrees-to-buy-sikorsky-for-9-billion-1437392758`

- **Threat Landscape** - OPM breach:

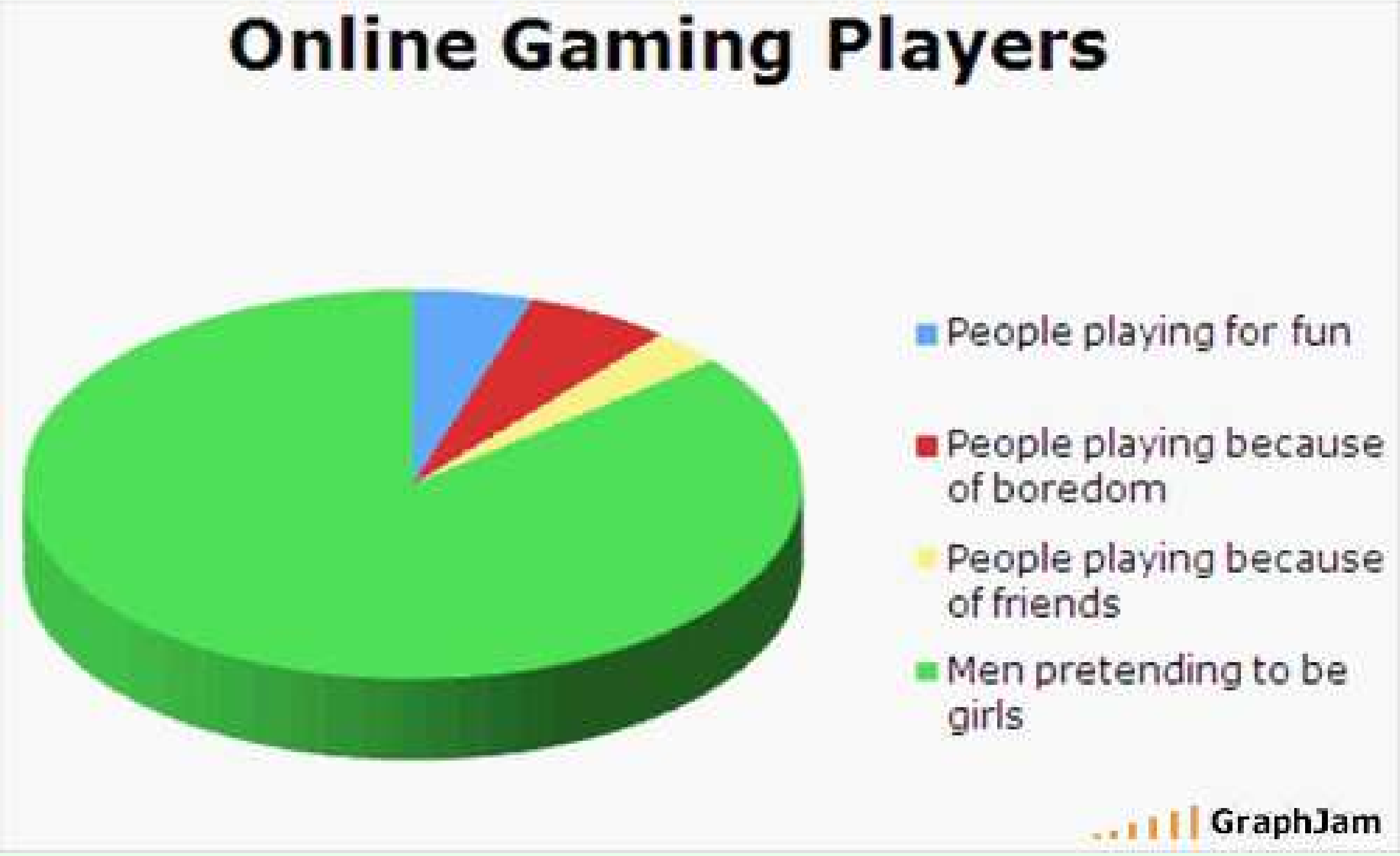
  `http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/`

Absolute certainty **doesn't exist**. Consider factors as contributing to increased or decreased likelihood of outcomes. Define what risks will be in or out of scope.

I am highly confident that the risk of misuse of OPM information about employees is likelier now than it was in 2013

Perception versus Reality

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks



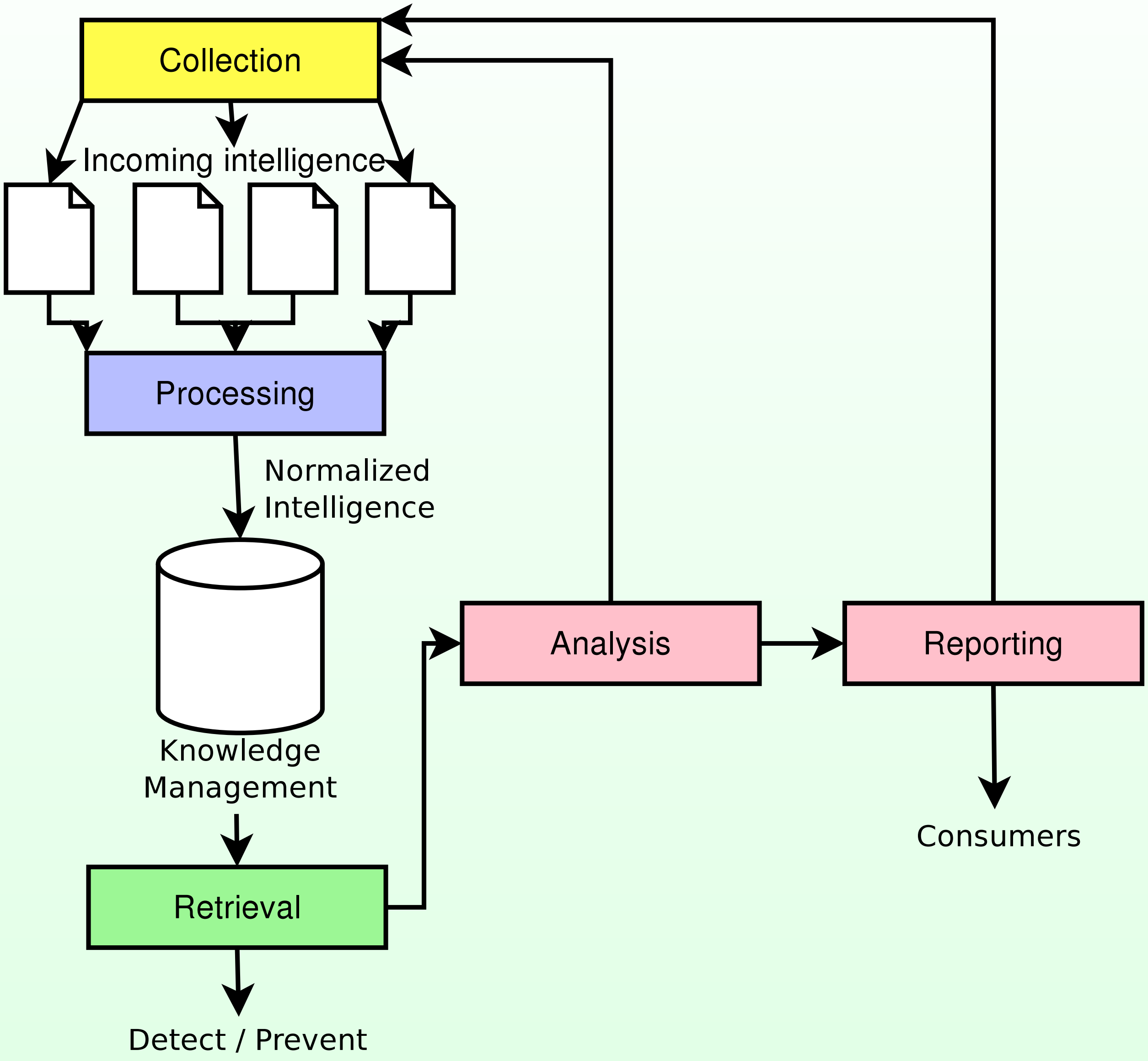
Affecting Confidence

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

- Some information sources more reliable than others
- Deeper investigation into evidence typically increases confidence, however also increases delay to reporting
- Age of evidence typically lessens impact on certainty
- Detail of evidence can help identify situational contexts for which evidence is higher confidence ("*IP is bad*" vs. "*IP is bad when observed sending email*")
- Quantity of independent sources supporting/refuting conclusion
- Quantity of sources with conflicting/competing assessments

A Cyber Intelligence Program’s Components

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks



Program Goals

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

Intelligence Consumption: Collection

Collection

- What sources to collect from (and not)?
- What scope do you consider?
- Decision driving information? → Structured metadata
- Technical vs. Informational: Audience
- What internal capabilities do you have to action? Tool survey

Your **Collection Plan** consists of what information you choose to inform your program, as well as identifying language in that information that will be most critical to inform decision making.

- Do you use Snort (`http://www.snort.org`)? If not, then intelligence in the form of Snort signatures may be something you want to exclude.
- CriticalStack Intel for Bro (`https://intel.criticalstack.com`): UI for creating custom collection plans. Bro-centric (`http://www.bro.org`).

Intelligence Consumption: Processing

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

Processing: Movement of data or material towards a known goal or end result, by passing it through a series of stages or a sequence of actions. Convert our raw material, the selected intel defined by collection plan, and run it through processing to normalize the information for inclusion into our knowledge management function.

- Read the narrative
- Document the relationships between significant data points
- Note important contextual clues (used in data theft? ransom? DDoS?)
- Attack models such as "Cyber Kill Chain" can be helpful for context
- Organize into consistent structured output, for storage. Always store original source document(s) and include references to them in output

Spreadsheets / CSV as output can be surprisingly effective

Intelligence Consumption: Knowledge Management

Your program's intelligence in its *final form*

- Program's intelligence is published for broader audience
- Queryable
- Normalized → consistent → predictable
- Once organized, it becomes easier to reorganize
- Old raw collections are easy to search/retrieve. Periodically re-process old intelligence as program matures

The organization of this system is driven by two factors:

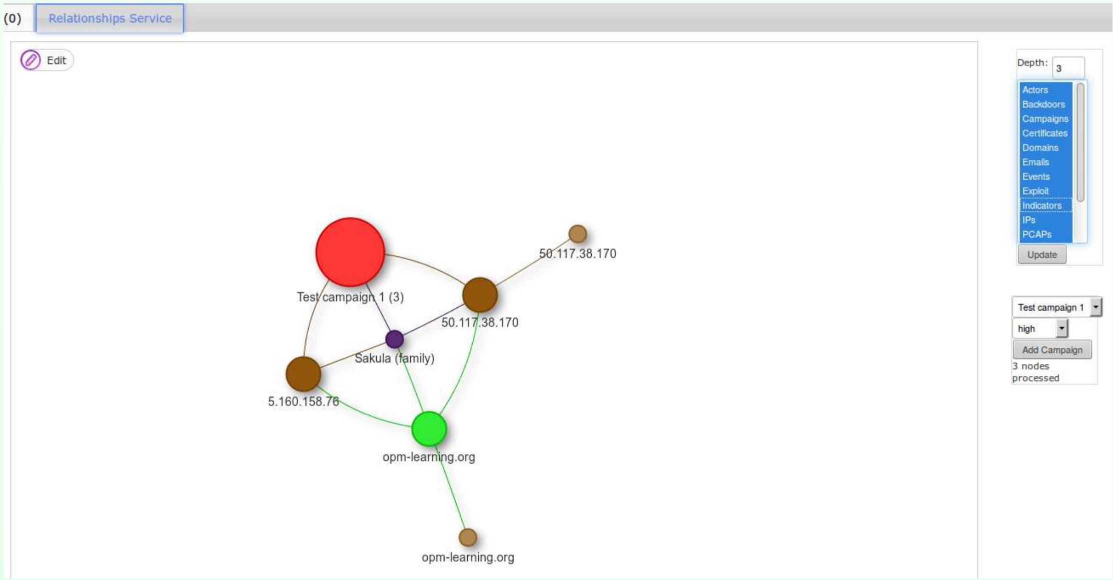
- Minimize pivots and external investigation by event analysts (regular feedback to drive this)
- Support dynamic signature deployment, using queries on collected context, with minimal tool-local modifications chasing each new collection

Intelligence Consumption: CRITs

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

CRITs: `https://crits.github.io`

- Open-Source, strong community support (developed by Mitre, contributors include GE, Ashland Inc., and growing)
- MongoDB helps support frequent collection plan changes
- Start with *something* to build from, rather than scratch



Depth: 3

Actors, Backdoors, Campaigns, Certificates, Domains, Emails, Events, Exploit, Indicators, IPs, PCAPs

Test campaign 1

high

3 nodes processed

Intelligence Analysis

Researching your collected intelligence to produce further intelligence that can be leveraged by your program.

Examples:

- Search for network indicators buried in lists of strings from EXEs
- Look across collected IP addresses associated with Corkow malware to identify network subnets containing 5 or more distinct IP addresses used for Command & Control
- Gather domains associated with "APT28 campaign" (FireEye), to identify WHOIS information which is exclusively used for domains by that group

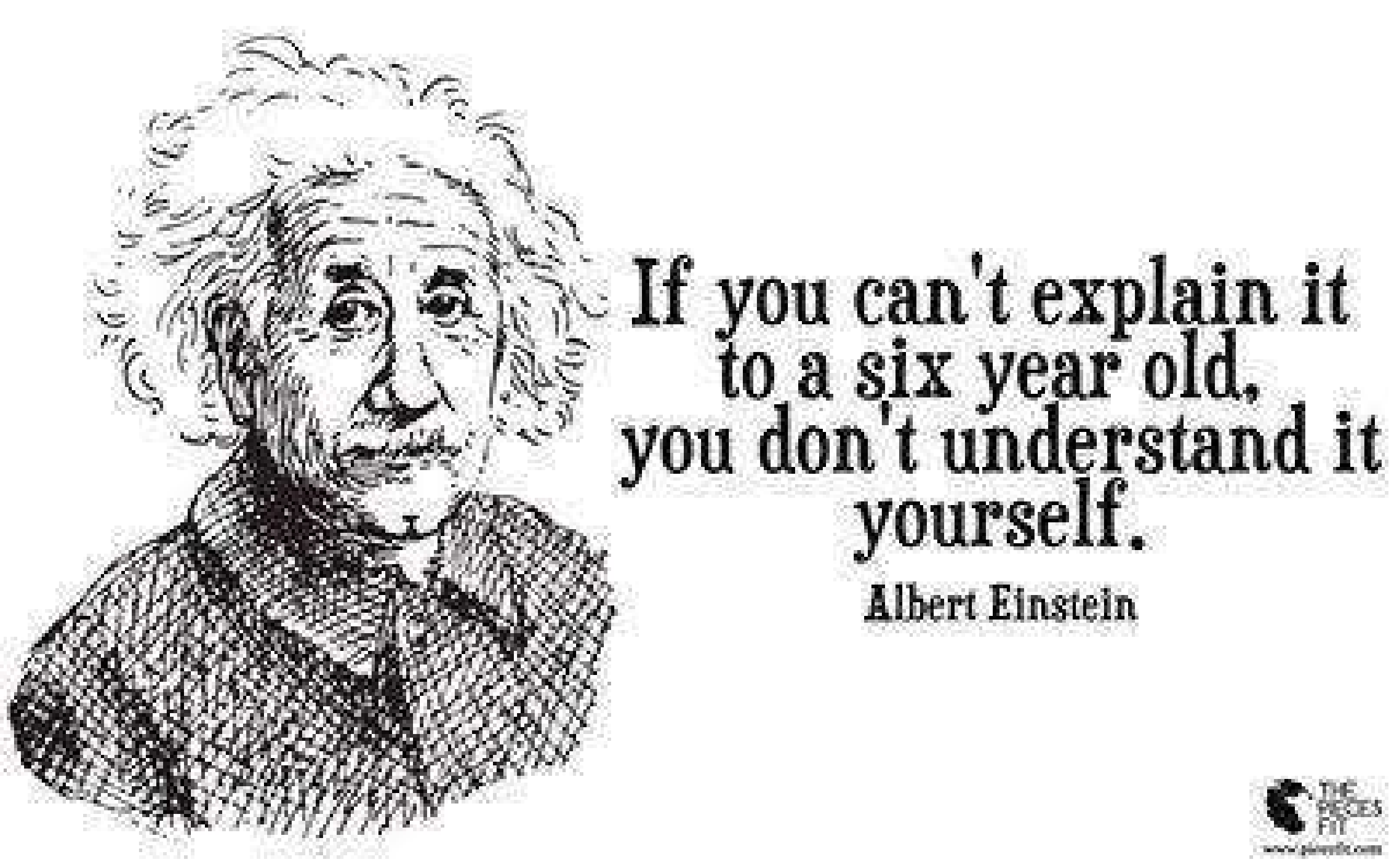
Preferred approach is to publish an internal analysis report, documenting conclusions with supporting evidence, and meeting as many collection requirements as possible in your narrative.

Feed the publication through your existing intelligence process:
Eat your own dog food

Intelligence Reporting: ELI5

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

Explain Like I'm Five


If you can't explain it to a six year old, you don't understand it yourself.
Albert Einstein
THE PIECES FIT

Intelligence Reporting

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

Can be treated similarly to *Analysis*, however also intended to inform an audience outside of your security team. Summarize away deep technical details, but also consolidate information from Analysis references into the same report.

Inside security team, treat just like analysis publications:

- Simplifies program
- Helpful for training (your own team is in flux as much as the threat landscape)
- Queryable records for "Where and when have we reported this outside our team?"

Intelligence Deployment

Deployment of intelligence describes delivering data from knowledge management into instructions for your tools / systems to watch for it in your attack surface. Using metadata collected and processed above, you can define static queries to retrieve intelligence stored in your program appropriate for specific uses.

Example:

- Process lists of IP addresses from known DDoS attacks
- Non-optimal to deploy them into Snort alerts
- Use Bro or similar to log connection-level metadata into elasticsearch
- Deploy to automated elasticsearch query that can report a single alert documenting all activity after exceeding a certain threshold

Return all IP address values into a JSON list where the IP address in CRITs contains at least one metadata object of type "Historic Activity" who's value is "DDoS".

Intelligence Deployment

- /me
- Intro
- Certainty
- Perception
- Confidence
- Program Components
- Collection
- Processing
- Knowledge Mgmt
- Analysis
- Reporting
- Deployment
- Thanks

Intelligence Deployment Examples

https://www.bro.org/sphinx/frameworks/intel.html

https://www.elastic.co/products/elasticsearch

http://suricata-ids.org/

http://plusvic.github.io/yara/

Thanks

- Security BSides Cincinnati 2015
- `http://bsidescincy.org/`

- Security513 crew
- `https://github.com/Security513`

- University of Cincinnati, Cyber Security programs
- `http://www.uc.edu/academics/cyber.html`