27th ANNUAL

FIRST BERLIN CONFERENCE

14-19 JUNE 2015

UNIFIED SECURITY:
IMPROVING THE FUTURE

VALIDATING & IMPROVING THREAT INTELLIGENCE INDICATORS

Doug Wilson

Threat Indicators Team, FireEye Labs

@dallendoug

#firstcon15

BACKSTORY

Measuring the IQ of your Threat Intelligence Feeds (#TIQtest)

Alex Pinto
MLSec Project
@alexcpsec
@MLSecProject

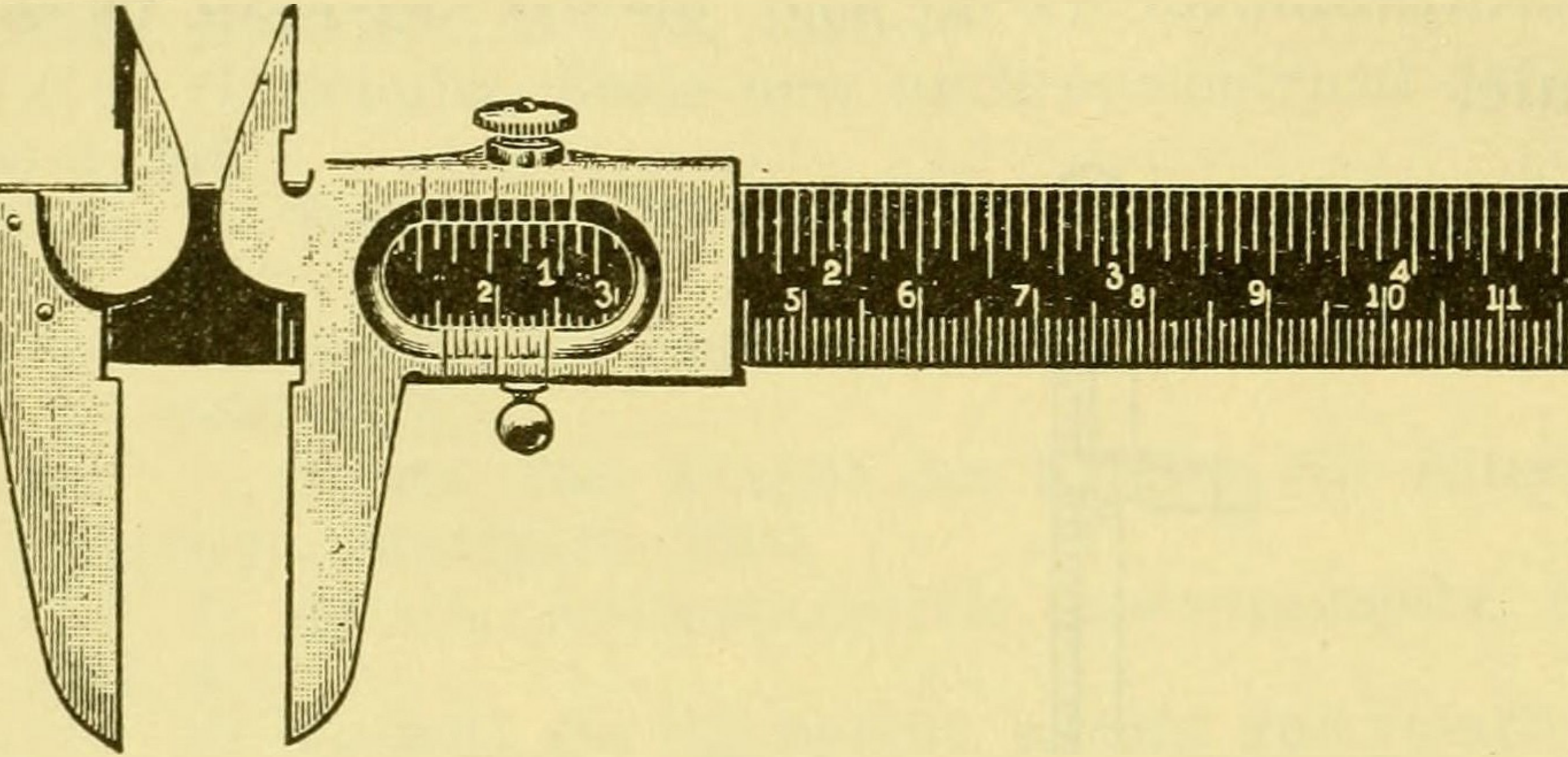
Kyle Maxwell
Researcher
@kylemaxwell

IP !~= IOCS

```
: MD5 is 81fd7555339242ef3b185907342f5bf1
: MD5 is 41122120170c5861552e3c2091d4d4e9
: Strings contains S3kretHiddenSTRINGz!

ile Compile Time is 2013-05-02T21:31:58Z TO 2013-05-02T21:33:00Z
ile Name contains evil
R
├── File Extension is exe
└── File Extension is dll
R
├── File Size is 61024
└── File Size is 63095
```

CAN WE MEASURE UP?



CONFIRMATION BIAS

WORDS WORDS WORDS

niccs.us-cert.gov/glossary

A-Z Site Map

CAREERS | NEWS & EVENTS | COMMUNITY | RESEARC

istpubs/ir/2013/NIST.IR.7298r2.pdf

NISTIR 7298
Revision 2

Glossary of Key Information Security Terms

Glossary of Common Cybersecurity

con is intended to serve the cybersecurity communities of practice and interest
complements other lexicons such as the NISTIR 7298 Glossary of Key Informat
are to enable clearer communication and common understanding of cybersecu
d annotations on the definitions. The lexicon will evolve through ongoing feedba

Homeland Security Office

NPPD Risk Management & Analysis

the
ke
levant to
analysis.
epartment
rt
S Risk

Lexicon:

- Promulgates a common language to ease and improve communications for the Department and its partners;

- Media Contacts
- Multimedia
- National Terrorism Advisory System

ARTIFACTS (NOUN)

A product of artificial character (as in a scientific test) **due usually to extraneous** (as human) **agency**

–Merriam Webster

INDICATOR (NOUN)

1. (noun) **A sign that shows the condition or existence of something**
2. **Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack.**
3. **A sign that an incident may have occurred or may be currently occurring.**

INDICATORS (OF COMPROMISE)

1. **Specific artifacts left by an intrusion/forensic artifacts of an intrusion that can be identified on a host or network**
2. **Greater sets of information that allow for the detection of intrusions or other activities conducted by attackers.**

COMPONENTS

- Data points
- Artifacts
- Indicators
- TTPs
- Campaigns
- Threat Groups

SIMPLE > COMPLEX

- Data points
- Artifacts
- Indicators

Simple

- TTPs
- Campaigns
- Threat Groups

Complex

EASY TO MEASURE

- Data points
- Artifacts
- Indicators

Simple

- TTPs
- Campaigns
- Threat Groups

Complex

MEASURE WHAT YOU KNOW

You can measure simple!

STATISTICS 001

	Condition TRUE	Condition FALSE
Test Result TRUE	**TP (True Positive)**	**FP (False Positive)** also known as **Type 1 Error**
Test Result FALSE	**FN (False Negative)** also known as **Type 2 Error**	**TN (True Negative)**

DETECT VS. INVESTIGATE

ARTIFACTS ARE EASY

1.2.3.4

45c3c85aca7d490c06ab14b811852f0b

Evil.exe

HKLM/BadRegKey

SO, HOW WOULD YOU TEST...

OR

processName = “Evil Running Process”

regKey = HKLM/MoreBadRegKey

AND

fileName = Windowsfile.dll

NOT fileMD5 = 45c3c85ac . . .

NOT fileMD5 = 14b811852f . . .

INDICATORS ~= CODE

Indicators are a program to find evil.

Properly written code performs as expected.

Bugs cause unexpected results.

	First Run	Second Run	Third Run
Samples	10	10	10
TP Detections	7	9	8
FP Detections	0	2	0

SYNTHETIC TESTING

SYNTHETIC TP TESTING

What to test on

1. **Stockpile of “evil”**
    - **Binaries**
    - **Web-shells**
    - **Intermediate files (Java, Flash, .Net)**
    - **Pcaps**
    - **Suspicious Utilities**

SYNTHETIC TP TESTING

What to test with

1. **Static detection rules**
   - YARA
   - Hashing & other File Analysis
2. **Network detection rules**
   - Snort
   - Network Parsers/decoders
3. **Execution and Behavioral detection rules**
   - Sandboxes Galore

SYNTHETIC TP TESTING

How to test

1. Create Test Harnesses
2. Determine Tolerance for FPs
3. Run Known Evil vs Rulesets
4. Examine Results

HOW TO DO SYNTHETIC TP TESTING
continues

5. Update Rules
6. Update Evil
7. Re-Run
8. Repeat

YOU'LL HEAR THIS AGAIN

Stay Flexible.

Change based off of results.

Sometimes you start measuring to figure out what you need to measure.

Make sure your systems can change/evolve.

SYNTHETIC FP TESTING

What to test on

Instead of detecting the evil,

now you want to NOT detect the good

SYNTHETIC FP TESTING

What to test on

“Clean” environments of all your above scenarios.

FP testing is HARD

Because you can’t model the entire internet.

SYNTHETIC FP TESTING

What to test on

Model as much as you can.

Accept you will miss something.

Make sure you have a feedback loop from “real” testing available.

SYNTHETIC FP TESTING

How to test

1. Create environments.
2. Create sets of user actions.
3. Use TP Rules and hope for NO hits.

HOW TO DO SYNTHETIC FP TESTING continues...

4. Update Rules.
5. Update Environments.
6. Update User Actions.
7. Re-Run.
8. Repeat.

SYNTHETIC TESTING OVER TIME

1. **Don’t just test, test over time/changes**
2. **Regression testing model**
   - Treat rules as source code
   - Treat detection efficacy as how well the program executes
3. **Make changes? Test again!**
4. **Change variables? Test again!**
5. **Study changes over time to learn . . .**

REAL WORLD TESTING

“REAL WORLD” TESTING

1. **TP testing & FP Testing are still your primary concerns.**
2. **Realize you control a lot less and have to assume a lot more**
3. **SET EXPECTATIONS**
    - Be prepared to be flexible.
    - If you are doing it wrong, change it up.
    - Make sure your system allows for this

MARK WITH CHALK, CUT WITH AXE

1. **Real world testing involves having a baseline**
    - You CAN get that from synthetic testing, and that's a good start. However, there are no guarantees
2. **Measure**
    - What rule hit
    - What it hit on
    - Validity of a hit (sounds simple, right?)
3. **Make SURE you get feedback**

ASIDE - RATING INDICATORS

Confidence & Criticality . . . ???

MEASURE WHAT YOU DON’T KNOW

SOURCE BOSTON 2015

Who Watches the Watchers? Metrics for Security Strategy

Michael Roytman

risk.io

Security Metrics are often about the performance of information s
centered around vulnerability close rates, timelines, or criticality r
are the rights ones? How does one measure risk reduction, or ho
operationalizing that which is necessary to prevent a breach.

SECOND ORDER EFFECTS

HARDER TO MEASURE

- Data points
- Artifacts
- Indicators

Simple

- TTPs
- Campaigns
- Threat Groups

Complex

EXPERIMENT!

Use your more abstract TI to power your deployment of Indicators and more easily measurable components.

(ASIDE) WHY NOT JUST DETECT EVERYTHING?

1. **In a perfect world, we would detect everything.**
   - However, everything is a lot
2. **Good/Fast/Cheap, pick two**
   - Ultimately, some limitation of technology or budget means that you can’t look for “everything” even if you knew what everything was
   - Sad but true state of affairs.
   - You’ll be a lot happier if you realize this limitation

TRENDS ARE FRIENDS

1. Collect data over time
2. Determine trends where possible
3. Use anomalies as a reason to review

THIS IS THE REAL WORLD

1. You MUST use feedback
2. You MUST be flexible
3. Realize sometimes the first result of measuring is to realize what more you need to measure
4. Look at what you DON’T have as much as what you do.

IF YOU SHOW ME YOURS, I'LL SHOW YOU MINE

MEASURING WHAT OTHERS HAVE

Peers, Vendors, and Sharing Relationships

SHARING != CYBER CARING

SHARING IS CONTROLLED COLLABORATION

TYPES OF COMMUNITIES

These might be symmetrical

Government < > Same Government

Industry < > Same Industry

Vendors < > Vendors

TYPES OF COMMUNITIES

These NEVER will be symmetrical

Government < > Other Government

Government < > Protected Citizenry

Industry < > Dependents

Vendors < > Customers

More Mature <> Less Mature

TYPES OF MOTIVATIONS

Making things “more secure”

- Your own Entity
- Specific Entities
- Your community
- And on . . .

TYPES OF MOTIVATIONS

Gaining Something Else

- Financial Profit
- Reputation
- Bargaining power

DIFFERENT MATURITY
DIFFERENT CONTRIBUTIONS

No Threat Intel powerhouse?

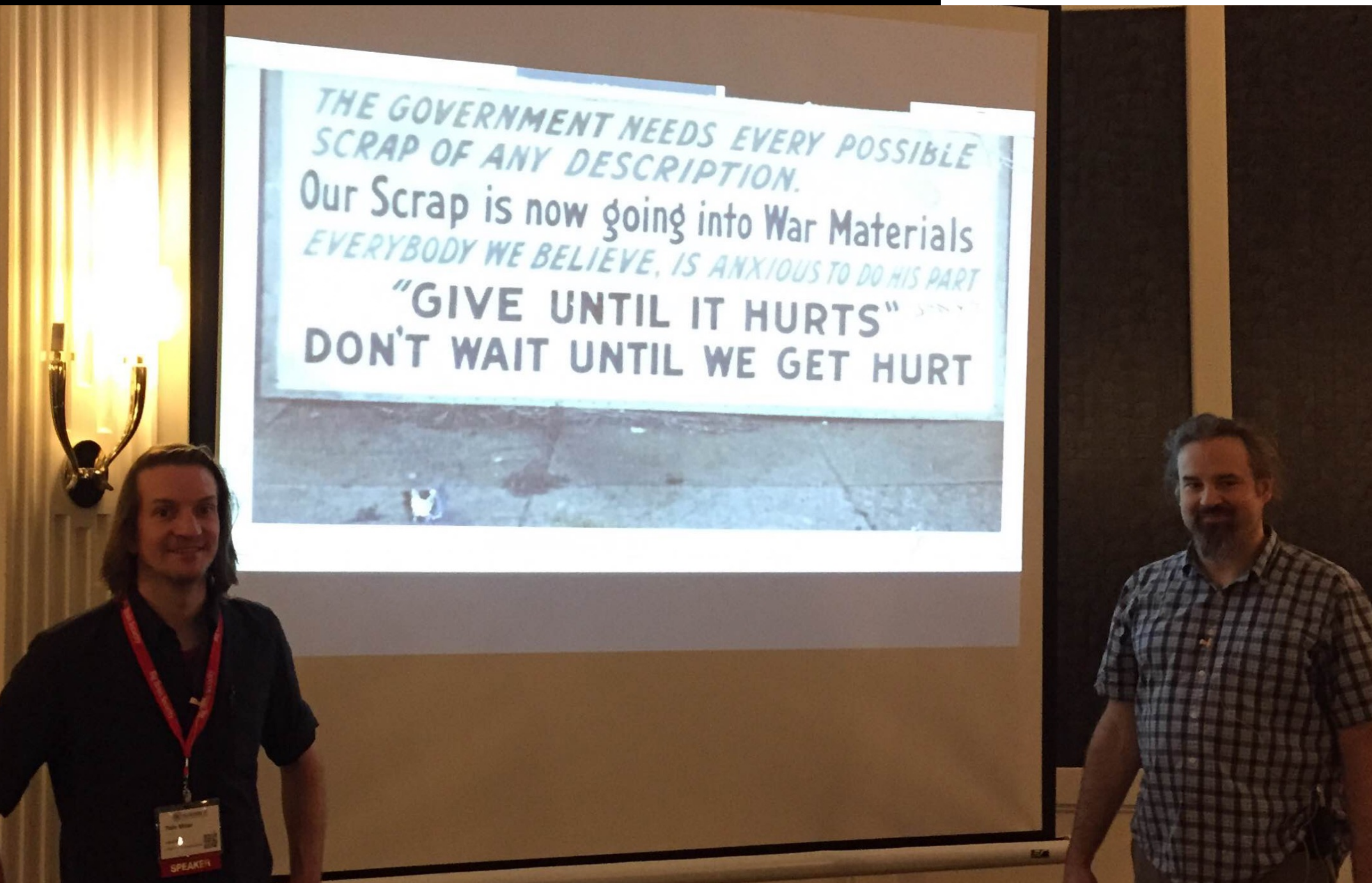
Supply

- **Data**
- **Testbed**
- **Feedback**

IS THREAT INTEL RIGHT FOR YOU?

1. **Basic level of security maturity needed**
   - before an Intel practice has any use
2. **Do you have:**
   - Insight into what is happening on your network
   - The ability to take action to control what is happening on your network
3. **If not, Threat Intel is NOT for you, yet. . .**

IT’S OK TO CHANGE YOUR MIND



DIFFERENT MATURITY
DIFFERENT CONTRIBUTIONS

No Threat Intel powerhouse?

Supply

- **Data**
- **Testbed**
- **Feedback**

WITHOUT FEEDBACK IT'S JUST PUBLISHING

GOALS AND MEASUREMENTS

Community with indirect profit motive

- Quality/breadth of Intel is going to be more limited
- Transparency will likely be higher
- Trust is less required for content, more required for membership

GOALS AND MEASUREMENTS

Community with direct profit motive

- Quality/breadth of Intel is going to be greater
- Transparency will be lower
- Trust is more required for content, and less required for membership

$64,000 QUESTION (OR MORE!)

So, can you answer the question of how to measure a vendor's Intel?

- In most cases Vendors will be participating in the less transparent communities.
- You CAN apply the second order observation ideas

$64,000 QUESTION (OR MORE!)

You can also

- Observe how an entity generates their Intel
- Ask how THEY measure their Intel
- And determine your trust level with the entity in question

IN SUMMATION

1. **The simpler TI is, the easier it is to measure**
2. **However, “Real” TI is pretty complex . . .**
3. **Any TI methodology should include**
   - Synthetic and Real testing
   - First and Second Order observation
   - Mandatory Feedback
   - And an ability to Adapt!

OTHER POINTS TO PONDER

1. You can engage in Threat Intel even if you are not super mature in Infosec
2. Sharing is Controlled Collaboration
3. Identifying what motivates collaborators is what will make sharing work

Don’t base your venture on a plan, Instead base it on a strategic foundation

You can have a plan, but know that it will change, probably a lot.

The plan is fluid, the foundation stable.

— Eric Schmidt, Google

QUESTIONS?

Doug Wilson

douglas.wilson@fireeye.com

@dallendoug

www.github.com/fireeye/iocs

www.fireeye.com

VALIDATING & IMPROVING THREAT INTELLIGENCE INDICATORS

Doug Wilson

Threat Indicators Team, FireEye Labs

@dallendoug

#firstcon15

27th ANNUAL

FIRST BERLIN CONFERENCE

14-19 JUNE 2015

UNIFIED SECURITY:
IMPROVING THE FUTURE