Organization Development With Bro

The Analyst Manifesto

Adam Kniffen

adamknifen@gmail.com

https://github.com/akniffe1

@adamkniffen

Life:

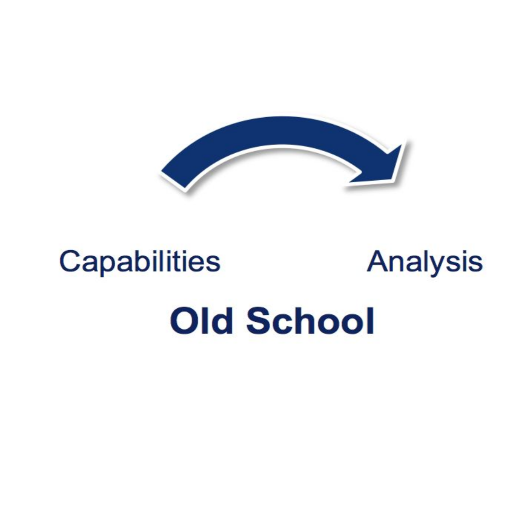
A house/battleground where the humans and cats are evenly matched, and the victor doesn't matter because the raccoons will eventually take over anyway.

Why the soft topic?

It’s getting weird out there:

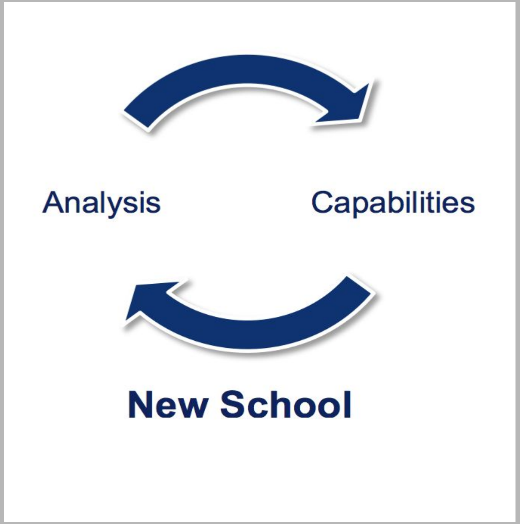
- Big Data Machine Learning Artificial Intelligence Anomaly Detection?
- “Data Lakes” ¯_(ツ)_/¯
- Classic Russian Information Operations in the News again
- The “Cyber Skills gap”
- Signature based detection is driving the industry again… by a different name

/wave Jason Batchelor and Mike Poddo


Capabilities

Analysis

Old School


Analysis

Capabilities

New School

Technology Can Radically Alter a Profession

- (Bad) Powerpoint and military leadership

- (Good) Composites and the Aerospace industry

- (Good) Remote Sensing and Environmental Sciences

- (Good?) UAS/Drones and the Intelligence Community

The Three Points of the Analyst Manifesto:

- Security is a knowledge building system
- Systematic collection and storage is the backbone of a successful security operation
- Analysis drives operations, tools, and technology

These Topics Are Driving The Industry... Why?

- "Threat Intelligence..."
- "Big Data... Machine Learning... Artificial Intelligence..."
- "___X___ Automation"

Security Is a Knowledge Building System

Knowledge > Information or data: Knowledge is vetted, contextualized, and useful for decision making

Knowledge can’t be assimilated, it must be built. Like all construction, it is a process.

Systems Theory: We need to focus on the activities and processes that most impact the entire ecosystem we’re working in

The knowledge we’re really after:

- What is Our Environment?
- How should the defensive organization function?
- What are my threats, and how do I manage them?

There are no shortcuts to answering these questions with any degree of confidence

The best activity for building knowledge on these subjects is to perform analysis: thus anything that enables accurate, well reasoned analysis is critical to success

The Security Knowledge Growth Curve

1. What do we do now that something happened?
2. What really happened?
3. How did it happen and what does it mean?
4. What are we doing now, how can that be threatened, and what happens with the rest of my defensive system if the threats become reality?

Effective Collection and Storage is the backbone of a Security Operation

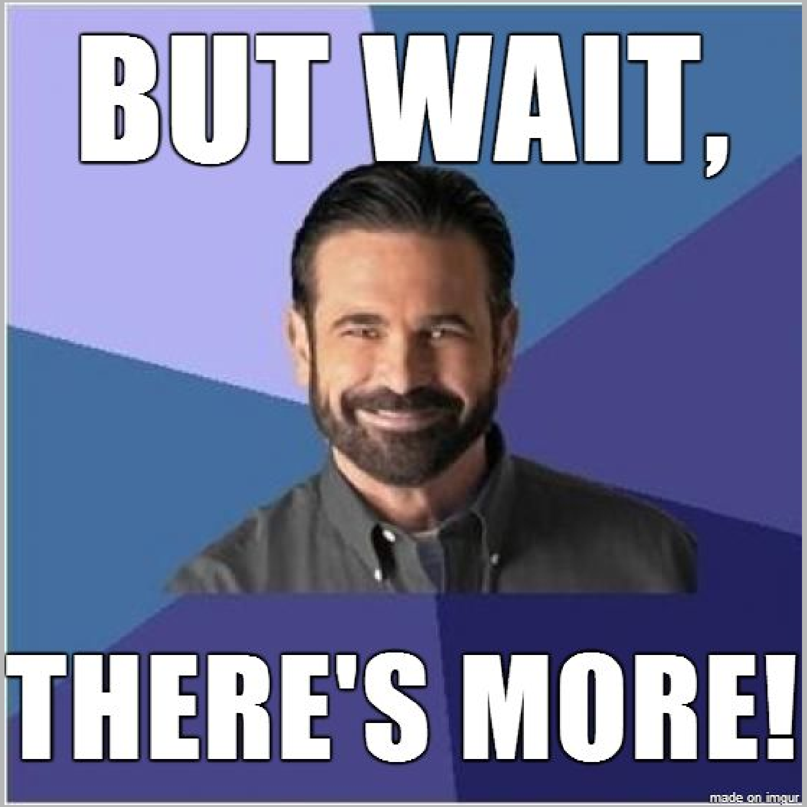
What’s the number one complaint from IR Dudes?

- I need the rights to do __X__
- I need __X__ software / server to do my job
- Dim the lights
- YOU CHANGED THE FIELDNAMES ON __X__ INDEX!
- I need visibility!

Visibility is good…

What happens when you have to post process an event to get to the detection opportunity you're looking for?

- Files
- SMB Commands
- SMTP logs



Achieving Parity:

What you learn through manual examination had better be deployable everywhere that matters, and accessible by everyone that matters.

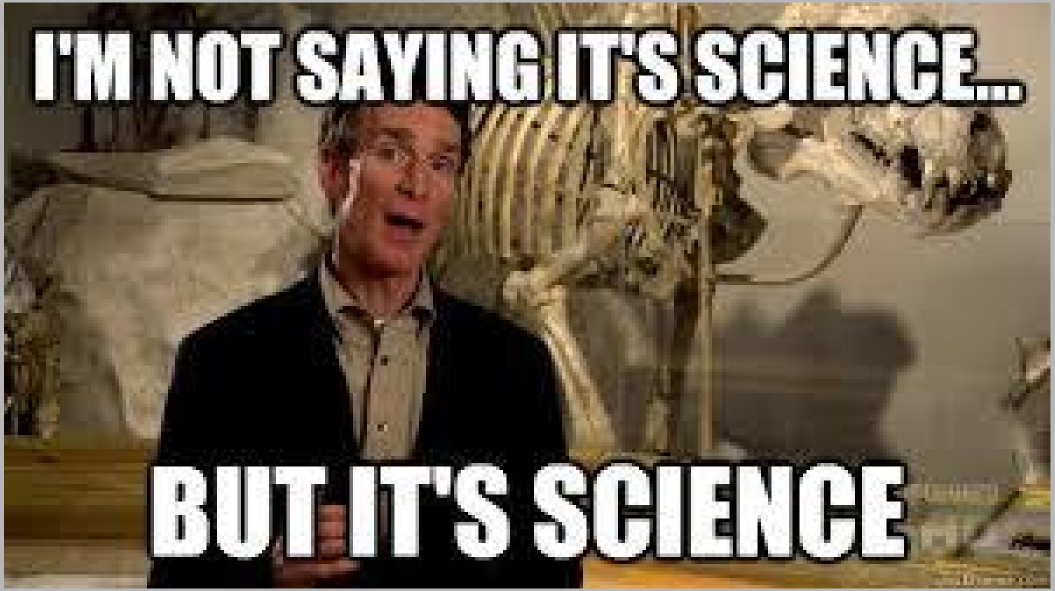
Simple Storage and Retrieval Requirements

- User defined saved searches and alerting opportunities
- REST API first, then Web UI
- **Aggressive** schema/indexing format enforcement
- >= 90 days of storage!
- Plan for extensive adhoc retrieval! IOW don’t sacrifice UX

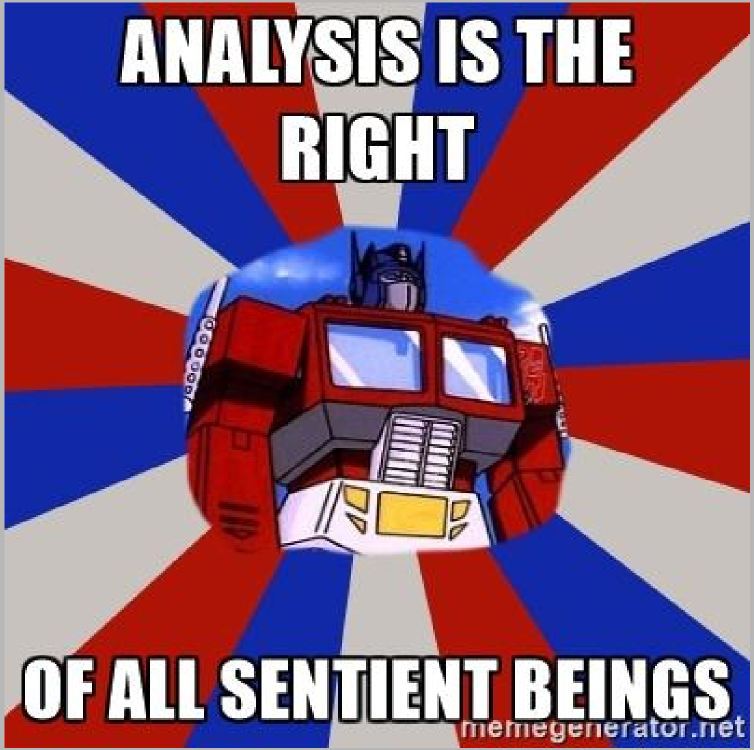
Analysis Drives Operations, Tools, and Technology!

What is Analysis?

- Make a hypothesis
- Perform tests against the hypothesis
- Examine evidence from the test
- Share the method and findings with others



Who Does Analysis?



The HR rep (and most titles) are wrong, Optimus Prime is right.

If everyone is doing analysis, what the !?^& do we manage?

The Hard Stuff!!!!

- team culture and dynamics
- Organization Structures, Responsibilities, Authorities
- Time
- Tools necessary to conduct research

Won’t we be powerless to __X__ attack if we don’t buy __Y__ appliance?

- Chicken VS Egg == dumb question
- Better Question: What do we know about __X__? If we know nothing, maybe we need to focus on buying content or making better friends (with NDA’s!)

You’ll only know if you do the research

Bro to the rescue?

The Security Knowledge Growth Curve

1. What do we do now that something happened?
2. What really happened?
3. How did it happen and what does it mean?
4. What are we doing now, how can that be threatened, and what happens with the rest of my defensive system if the threats become reality?

Bro Helps! (by the levels)

Level 1 -2

connect the dots between sensors and controls and build your own IOC/IOA from vendor “decisions”

low barrier to entry (buy / build with help)

Level 3

Network TiVo! Rewind events outside PCAP index thresholds

(generally) extensive documentation of analyzers and code base--there are few mysteries

Level 4

HUNT!

Tag critical asset traffic and do things differently for that traffic

“Glass House”

Validate other tools telemetry

Bro 2.5 Can Really Help!

Level 1 -2

SMB logging helps you see ransomware lateral mvmt

Validate that you’re seeing the right traffic quickly with VLAN tags

Level 3

More precision on monitoring your sensor health and performance

Better, independant understanding into your email ecosystem

Level 4

Updated plugins for more options to control packet_loss

Expire indicators at the sensor==less confusion with indicator lifecycle

Identify and analyze rogue remote admin protos

Moving Forward!

Analyst Outreach / Influence

Storing Bro Data:

- Graphs
- Documented oriented Database
- Hybrid Databases

Highly Distributed and Zone based Sensors

Aiming the “log cannon”

Ze End:

Analyst Manifesto:

- Security is a knowledge building system
- Systematic collection and storage is the backbone of a successful security operation
- Analysis drives operations, tools, and technology

Bro’s greatest gifts:

- Comprehensive, detailed, and extensible telemetry
- Extremely flexible deployment and management
- A language for traffic analysis, and a bunch of highly vetted code that uses it
- An active development and operations community to grow with