"Can we leverage network monitoring to build comprehensive situational awareness of our operating environments in a way that scales well? How could such an awareness allow us to find anomalous and malicious behavior?"

SOURCEfire®

God I hope so.
If not, is anyone hiring?

**(Hi, I'm Matt Olney,
Senior Research Engineer,
Sourcefire VRT)**

SOURCEfire®

Step 0: Management Primer

- Spending all the money on the planet on hardware will not help you
  - Don’t tell sales and marketing I just said that
- Investment in your people will return a much greater dividend
  - Investment is time and money
    - Time to think
    - Money to learn
- Hire someone who knows how to evaluate technical talent
  - Because firing people is a pain in the ass
  - Don’t tell the people at this conference I just said you should fire people who aren’t really, really good at what they do

Step 1: Get a grip on your network

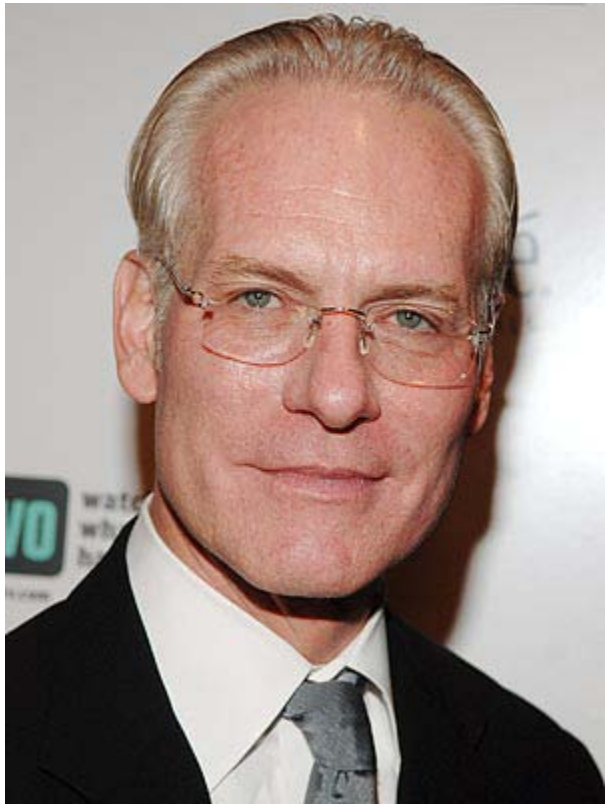
- Network Visibility
  - Netflow
  - SNMP Polling
  - Network Discovery
    - PADS
    - RNA/RUA
- Intrusion Detection
  - IDS/IPS
  - HIDS
  - AV
  - Whatever a Razorback is

Step 2: Make the set of tools a system

- Guns don't kill people, people kill people
  - That being said, having a good gun helps
  - I'm not sure if this analogy really went the way I wanted it to
- Matt's Tool Wish-list
  - Maximize your investment in your people by giving them tools that will support the skills and intelligence they bring to the table
  - Transparency
    - Minimal magic
  - Customizability
    - Rules language
    - Parsing definitions
    - Verbose, granular configuration
  - Extensibility
    - API/SDK
    - Allow me to rework your vision to come inline with my reality
  - Scalability
    - The ability to get output into a scalable SIM/SIEM/Data-Thingy delivers scalability for custom developed detection capability
- Razorback, released at DEFCON

Step 3: Make it work, people

- An object at rest tends to be useless
  - Blinky lights have never stopped an attacker
- Actively developing your detection stance:
  - Makes your detection stance more unique
  - Doesn't waste resources on capabilities that don't support your defensive stance
  - Defines what your tools do, not some monkey developer in a cube
- Pay attention when Cloppert gives his talk
- Matt wins for referencing Bravo



Step 4: Matt Wants a T-Shirt (XXL)

- APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT APT
- Sourcefire will sell you a Unicorn with a Delphic Oracle plugin that will foresee the coming of the APT
- Zeus plugin will allow for orbital laser strike (OLS) to remove APT threat at the source
  - Support contract for OLS for 5/10/25/Unlimited strikes per month
- Demoware Unicorn/Delphic Oracle platform available, limited to detecting APT from Burkina Faso
- http://volatility.tumblr.com/post/766031242/a-volatile-challenge-finding-the-apt-advanced