

➤ Information Security Decisions



Security Data Management: It's All About Visibility

Aaron Turner
Enterprise Security Partner
N4struct

Why Are We Here?

- You came to see me talk... So who am I?
- Professional standards for information security
- It's 2012... do you know where your data is?
- Tracking data – hard on the wire... wireless what?
- Prioritizing data visibility

Who is This Aaron Turner Guy Anyway?

- Long-time InfoSec... victim? ... participant? ... err...
- When non-technical friends ask me what I do for a living, I tell them that I'm an Internet Janitor & Hall Monitor
 - Clean up really big messes
 - Sometimes I've created big messes for the sake of testing out new kinds of cleaning supplies that we will need in the future
 - I've tried to track hackers and understand what they do and how they do it
- Smartphone reverse-engineer hobbyist and licensed spectrum communications researcher

So... You're an Information Security Professional...

Holding ourselves to professional business standards

- Our peers in the 'business world' are held to measurable results (P&L, growth, etc.)
- InfoSec has often been in the land of 'qualitative' or 'subjective' measurement

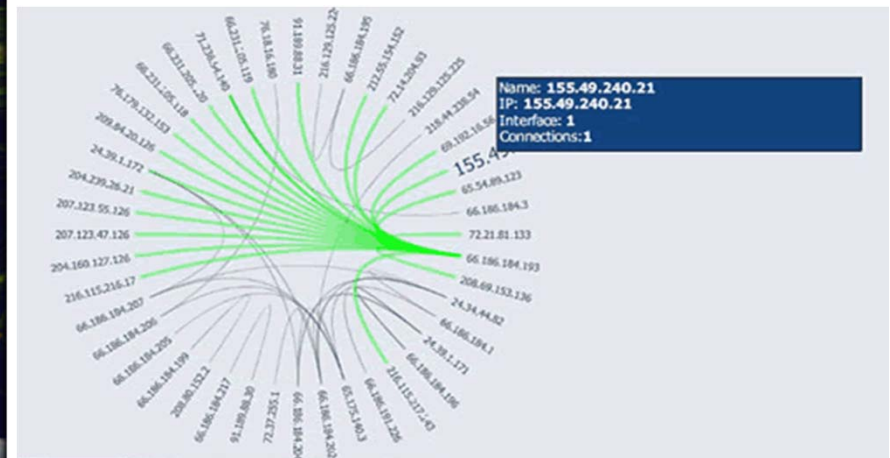


Establish a baseline for protecting information

- Start small (how many emails are flowing per day to/from one group)
- Move to global measurements (how many Facebook posts per day)
- Knowing what 'normal' is will be the only path to long-term success
- Properly vetting anomalies will improve your credibility with peers

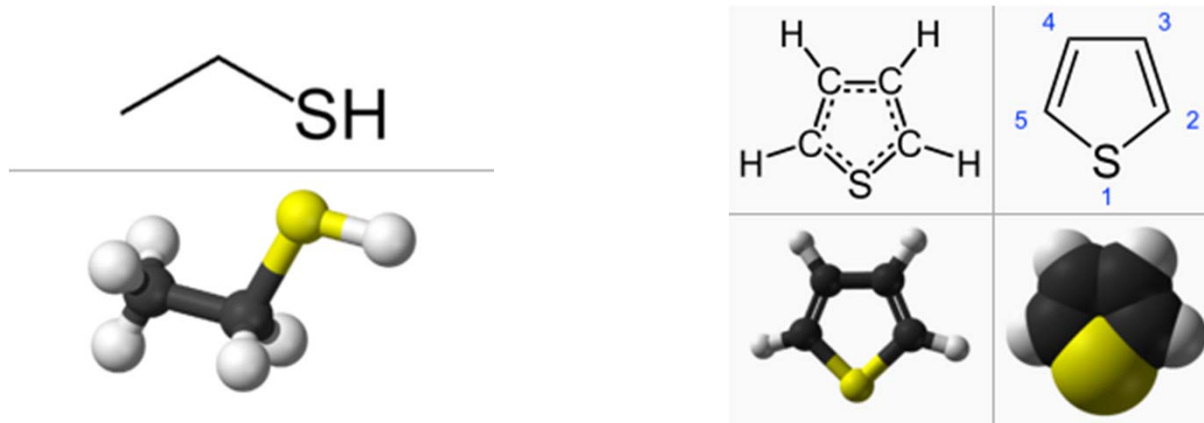
Data Route Mapping – Wired Networks

- Track data traffic patterns and volume
 - External NETFLOW baseline
 - Internal IP address correlation baseline
 - Connectivity baseline (VPN, MPLS, etc.)
- Who, what, when, where... all to help you with WHY



A Quick Break – Brought to You by Propane

- How to see the ‘un-seeable’?
 - A quick example... anyone know what these are?



- Ethanethiol & Thiophene
- OR...
 - What makes Liquefied Petroleum Gas stink!

How Can We 'see' Wireless?

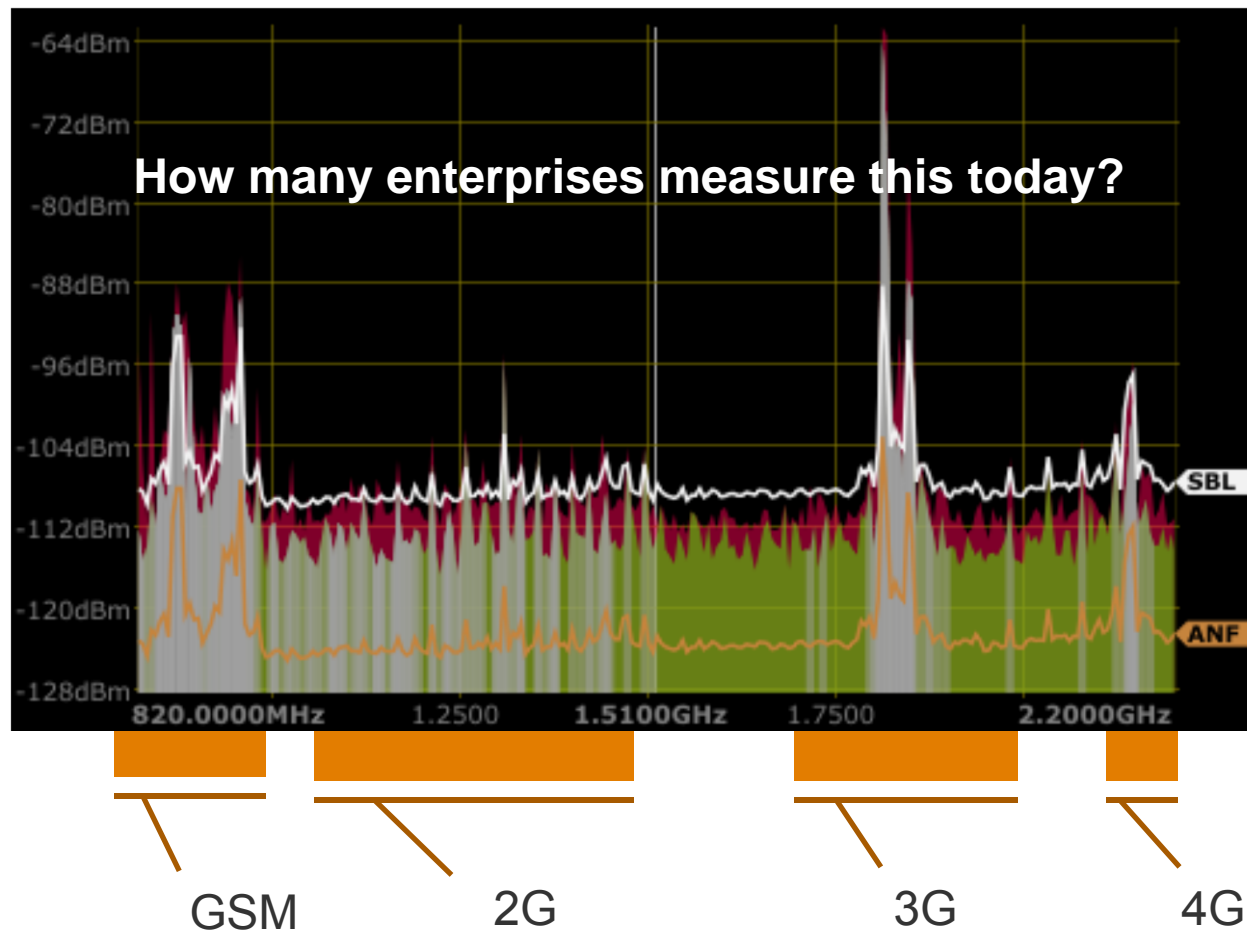


Used with permission – Timo Arnall – elastic-space.com

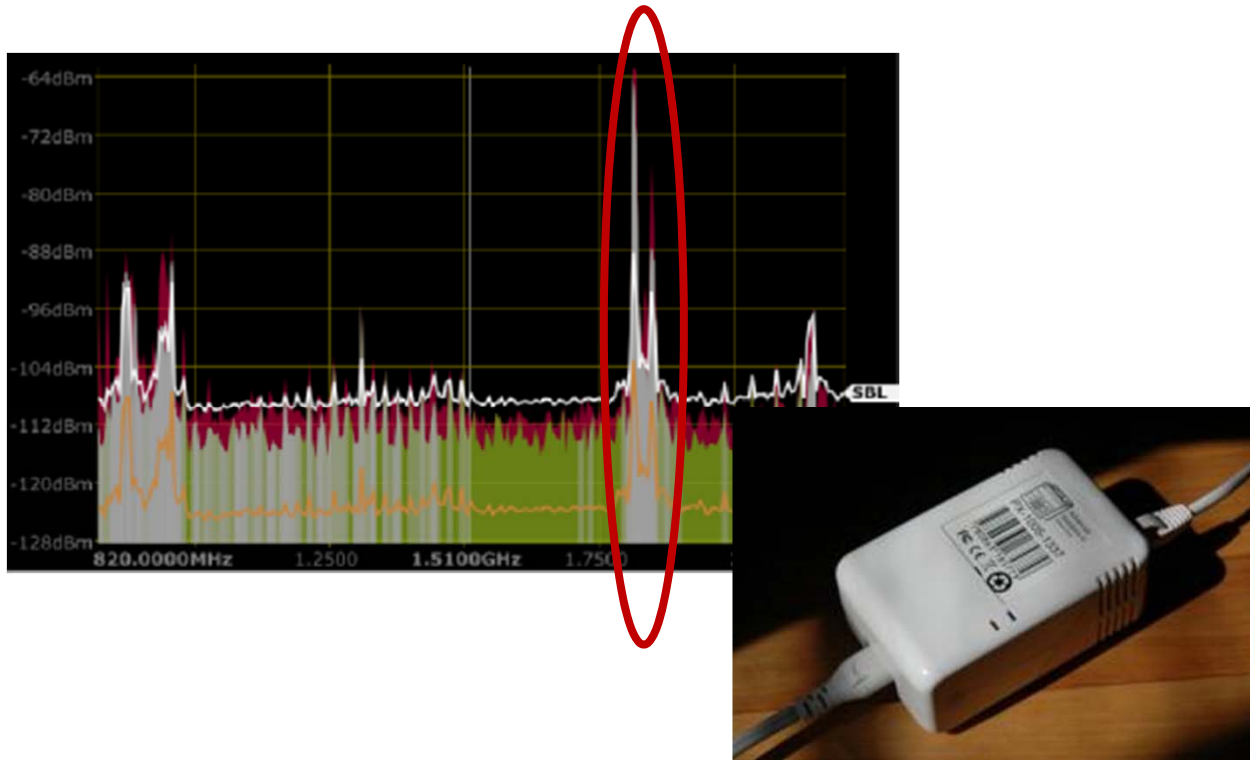
How Do We Visualize Enterprise Networks?



How Can We Visualize Licensed Spectrum INSIDE of Enterprises?

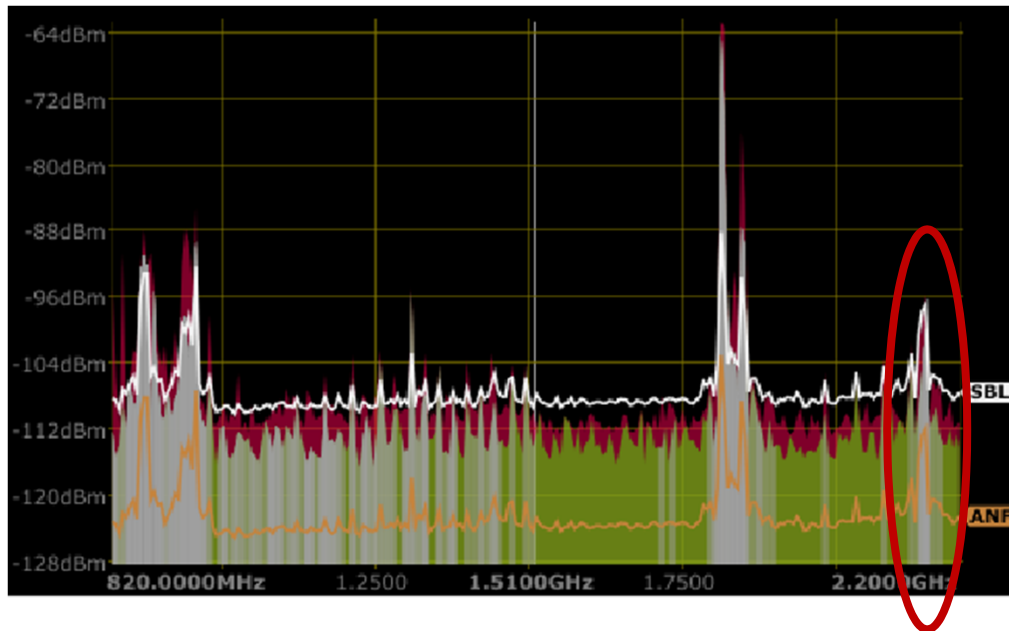


Recognizing Threats – 3G LAN Bridge



PWNIE EXPRESS

Recognizing Threats – 4G LAN Bridge




Without a Monitoring Plan...

- What does an 'normal' look like?
- If there were any anomalies, how would an enterprise know?
- Anomalies seen in the past year:
 - Cellular intercept equipment permanently installed at foreign offices
 - Portable cellular intercept equipment detected at US offices
 - Persistent cellular monitors installed on corporate-liable handsets which constantly 'beacon'

What to Do?

- Establish wired network data baselines
- Establish wireless measurement strategy
- Correlate wired with wireless
- Measure, measure, measure
 - Looking for anomalies can be hard, but is the only way to know what 'normal' is



Aaron Turner
Enterprise Security Partner
N4STRUCT



Featured Member of the
TechTarget Editorial
Speaker Bureau