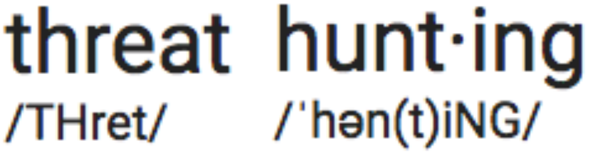
THREAT HUNTING

Or "Incident Response Warrantless Wiretapping"



threat hunt·ing

/THret/ /ˈhən(t)iNG/

A complex process of proactively and iteratively searching networks to isolate advanced threats evading security tools.

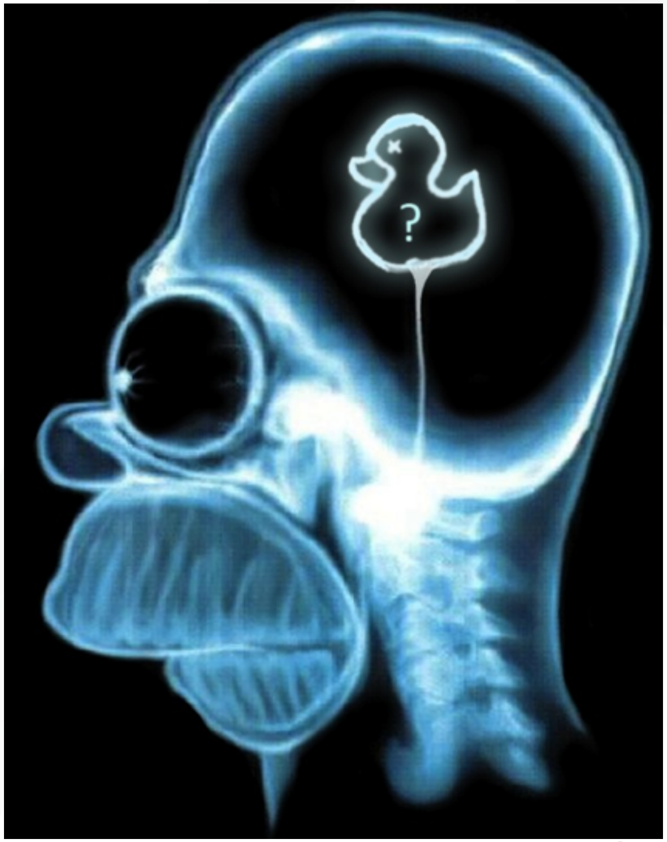
Threat Hunting is, at the basest level, Investigation without cause

THREAT HUNTING

- Hunting is active, methodical, and continuous.
- If you already know what you're looking for that's Searching; not Hunting.
- Threat actors must operate within your environment to be successful
  - Use your HOME-FIELD ADVANTAGE.
  - Similar to "Malware can hide but it must run" from memory forensics
  - Focus on Choke Points Attackers HAVE to Traverse
- Understand what traces are left (breadcrumbs or threads) from both the network and host perspective.
  - Locard's Exchange Principle
- Threat Hunting cannot be fully automated
  - Automation can help, but you need people to win against people

THREAT HUNTING MINDSET

- Assume a compromise
- Don’t wait for an alert
- Don’t assume someone else has seen this before
- Attacks are always changing
- **Know what bad looks like**
- **Know what normal looks like**



BENEFITS OF THREAT HUNTING

- Find previously undetected threats
  - Reduce dwell time (infection to detection)
- Learn the environment / dataset
  - Biggest ‘hidden’ ROI
  - Enhance speed and accuracy of response efforts
- Improve overall organization posture
  - Find misconfigurations
  - Identify Gaps
  - Reduced attack surfaces
- **Hunting Makes Analysts Better**
  - Puts Analysts in Front of Problems
  - Builds Investigative Mindset
  - Builds Technical Knowledge
  - Builds Organizational Knowledge
  - Solidifies Training Knowledge

THREAT HUNTING VS INCIDENT RESPONSE

- Similar methodology, skills, tools and techniques
- Different initial mindset
  - Hunting: Assume a compromise. Go find it.
  - IR: Prior knowledge of an compromise. (Initial thread to pull)
  - Steps after discovery are quite similar