Before we begin – a nod to the skeptics

Two categories of skepticism directed at yours truly

1. Skeptical that I am trying to sell you something
2. Skeptical that I CAN’T sell you something
To my skeptics: I AM NOT GOING TO/TRYING TO SELL YOU ANYTHING.

NO, REALLY.

(You can uncross your arms and expect less of me now.)
Threat hunting: The active process of looking for a threat in the absence of a previously identified indicator of compromise.
Before we go on – What it is NOT

• It's not a “new” practice
• It’s not a “special” practice
• It's DEFINITELY not all about technology
Why Threat Hunting?

TL;DR - IF YOU AREN’T, YOU NEED TO BE.
Common Questions and Challenges

Free consulting: All inclusive problem solving procedure. You’re welcome.
“I know – BUY A TOOL!! ”

Ummmm…. no.

(BTW – Free is powerful! Come see me afterwards and I will SHOW YOU.)
Since its not new – what is commonly known?

01
The same fundamental analysis skills used daily by security analysts are the ones needed to Threat Hunt.

02
Threat Hunting is a process – one that is linked to Security Operations.

03
That there are well documented approaches methods for guiding threat hunting activities.
Three generally accepted approaches – the “start”

1. Proactive
2. Hybrid Proactive
3. Reactive
On being purely “proactive”.....

“Big Data”
Normal
Expected/Not Expected
Problematic? (foreshadowing)

Threat!

Less Context
More Context

You better know what you are talking about
Refining “Problematic”

- Kill chain can help refine the hunting (It can HELP – some things can’t be easily seen)
  1. Proactive
  2. Hybrid Proactive
  3. Reactive

- Nod to Lockheed Martin and the Kill Chain
Doing Better…

• So, lets say you are busy doing other stuff.
• Maybe – MAYBE, being a one person army
• START WITH RISKS AND ASSETS!!! (NOTE: THIS MEANS WORK)
• All things are NOT equal
It’s ALSO a process, that said....

This is a great PROCESS OVERVIEW – REALLY! (Respect!!!!) It is, however, NOT a process!

https://taosecurity.blogspot.ca/2017/03/the-origin-of-threat-hunting.html
That ain’t a process.. THIS IS A PROCESS!
Even if you have a process…. (The six R’s)

If threat hunting is not:

1. Relatable to the business consumers
2. Repeatable (Consistency in favourable outcome)
3. Resilient (Outputs stand up over time)
4. Reliable (Provides consistent value to business)
5. Realized (Meaning not just talk – ACTUALLY doing it)
6. Realistic!

THREAT HUNTING WILL BE OF LITTLE VALUE TO SECURITY OPERATIONS

Make threat hunting a SERVICE!
1. Set Service levels and operating levels throughout the Threat Hunting

2. Create a mechanism for consistently conducting threat hunting

3. SET EXPECTATIONS!!
Awesome. Been great!
motto@lyricalsecurity.com
Stay strong, people!