Threat Hunting, Defined

Bamm Visscher
CIRT Manager, Cyber Defense
General Motors

April 12, 2016
$ whoami

Bamm Visscher (bamm@sguil.net)

- Husband, father, Michigander, camper, fisherman
- 19 years as an InfoSec Professional
  - USAF, Fortune 500s, and Fortune 10s
  - CIRT Operations
- Warning: I work from home
Threat hunting

[nthret huhn-ting]

da noun
1. the act of a person, animal, or thing that hunts

da adjective
2. of, for, engaged in, or used while threat hunting:
   a threat hunting cap

Origin of threat hunting
- Google says the term was popularized summer of 2011

Difficulty index for threat hunting

*Information security professionals are guaranteed to argue over the meaning of this phrase*
Real time analysis

- Information security operations
- Event driven analysis

The right way

- Analysts leverage their expertise to determine if alert was accurate, identify malicious activity, and if the attack was successful

The wrong way

- Triage only analysts
- Scope dopes / F8 monkeys
"If you have an alert problem, if no one else can help, and if you can find them, maybe you can hire the B-Team”

Pyramid of (Analyst) pain

- Atomic indicators can quickly overwhelm real time operations
- Performing regular analysis of IOC results over a period of time in bulk
- Must accept possibility of longer detect times of known IOCs
Threat Hunting

Leveraging information (threat actors, potential targets, IT infrastructure, etc.) to identify artifacts of a previously undetected compromise.

Into the rabbit hole we go....

- Threat hunting is an attitude
- Threat hunting has no expectations
- Threat hunting is NOT limited
- Threat hunting is NOT new
Conclusion

- Share with your teammates
- Share with your trusted partners
- Do not judge others’ techniques
- Teach others to threat hunt!
BRANDS THAT INSPIRE PASSION AND LOYALTY

Thank you
BRANDS THAT INSPIRE PASSION AND LOYALTY

GM