

RSA® Conference 2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: AIR-T10

THREAT HUNTING STRATEGY: HOW TO CATCH BEARS AND PANDAS

MODERATOR: **Dr. Anton Chuvakin**

VP Distinguished Analyst @ Gartner
@anton_chuvakin

PANELISTS: **Heather Adkins**

Director, Information Security and
Privacy, Google

Dmitri Alperovitch

Co-Founder and CTO, CrowdStrike

Craig Hancock

CISO, Telstra



Discussion Topics



- Can we *please* define THREAT HUNTING (TH) before we discuss it?
- Is TH only for very large companies with huge security teams?
- What are the practical pre-requisites for doing TH?
- How do you prove to your leadership that you need to TH?
- Can you actually "outsource" TH? Is this even conceivable?
- Describe your favorite TH success case!
- Lessons learned doing and organizing TH efforts



- ~~“The defender needs to close all holes, but the attacker needs to just find one hole to get in.”~~
- “The attacker needs to hide all his traces, but the defender needs to just find one trace to unravel the intrusion.”

CAREFUL!

OPTIMISM ALERT!!

Defender WIN!!!

So, What Is THREAT HUNTING...



- ... devoid of marketing fluff?

“Threat hunting is an **analyst-centric process** that enables organizations to **uncover hidden advanced threats, missed by automated** preventative and detective **controls**.”

It represents an *ultimate advanced (!)* security practice suitable for well-resourced security organizations facing persistent and stealthy threats.“

“How to Hunt for Security Threats” (G00327290)

Nicely Put



Dr. Anton Chuvakin  @anton_chuvakin · Mar 9

What are the most abysmally fake examples of totally NOT threat hunting that vendor(s) called "threat hunting"? [#question](#)

 17  10   31  



Robert M. Lee  @RobertMLee

@RobertMLee

Following 


Replying to [@anton_chuvakin](#)

If it's not a hypothesis led proactive investigation it doesn't fit. Also it has to go beyond your current automation footprint, so by default if a tool is doing it it's not threat hunting. But an analyst could use any tool to go on a hunt if it helps test the hypothesis

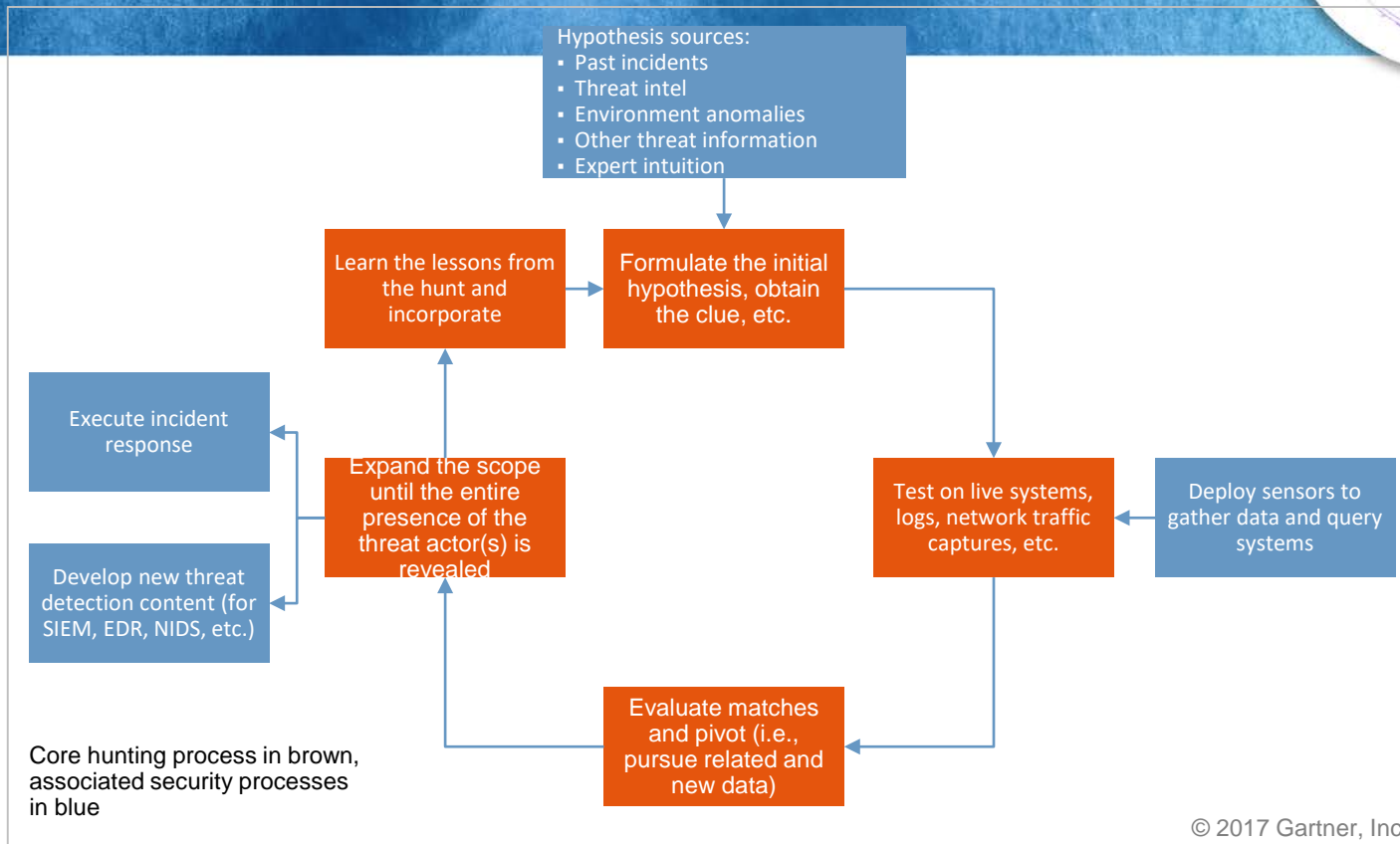
9:46 AM - 13 Mar 2018

13 Retweets **40** Likes



 5  13   40  

Foundational Threat Hunting Process



© 2017 Gartner, Inc.

Common Question: Where to Get Initial Hypothesis?



1. Threat intelligence – threat actor **capabilities**, primarily
2. Past **incident data**, indicators and attacker tools, techniques and procedures (TTPs)
3. **Red team and threat simulation** artifacts
4. Various environment **anomalies** – “what if this means we are hacked!?”
5. **Expert intuition** – yes, expert hunter intuition is often named as #1 source
 - Did we mention that TH is an ad hoc, creative process?

The Final Page: TH and Other Security Processes



Apply



- ✓ Don't try to hunt if you're still building lower-maturity detection and response capabilities. Improve detection and alert triage first!
- ✓ Build a business case for TH using preventing unacceptable incident losses by discovering advanced hidden attackers early, reducing incident loss and reducing security incident response costs.
- ✓ Start by conducting one hunt of several days' length, formalize ad hoc hunting already going on, or engage with a service provider promising "managed hunting."
- ✓ Use the cyber kill chain to structure your hunts around specific types of attacker activities in your environment.



- Falling for vendor's corrupt concept of hunting and getting something else entirely (#1)
- Reducing hunting to simplistic indicator matching
- You will find more evil and will have to respond – be ready!
 - Doing a hunt and then being overwhelmed by an attacker is not good...
 - Chilling lessons of 2018 IR: the good guys don't always win in the end!
- Threat hunting is hard to measure, because of its nature
- Too much reliance on hunting tools or any singular data type
- Failure to keep up with latest threat news/intelligence