WHAT WOULD YOU SAY YOU DO HERE?

Redefining the Role of Threat Intelligence
Rebekah Brown | @PDXBek

Intelligence Lead at Rapid7

But before that…

• Gunnery Sergeant United State Marine Corps
• Chinese Crypto linguist and Network Warfare Analyst
• Policy Developer
• Liaison to State and Local Governments
WHAT WOULD YOU SAY
YOU DO HERE?
THERE IS MORE THAN ONE WAY TO UTILIZE THREAT INTELLIGENCE
The Intelligence Process

Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)
Target

Needs, new information

Analysis: gaps, requirements

Information sources (collectors)

New information

Analysis: answers, actionable intelligence

Problem (customers)
WHAT DOES THAT MEAN FOR YOU?
Identify your focus area:

– Alerting
– Investigations
– Business Decisions
– Others?
Build a Collection Plan:
– What info do you need?
– What info do you have?
– Internal or external?
– What can you act on?
Evaluating External Sources

- Where does the info come from?
- What types of threat groups does it cover?
- What types of information does it include?
- Primary source or enrichment?
DON’T DISCOUNT OPEN SOURCE INTELLIGENCE!
Pick a Model:
- Diamond
- Target-centric
- F3EAD
- Your own?
QUESTIONS?

INFO @RAPID7.COM