RAPID7

HOW TO BUILD THREAT INTELLIGENCE INTO YOUR INCIDENT DETECTION & RESPONSE STRATEGY

Get CPE Credits for this Webcast

- Attendees of this Webcast are eligible for 1 CPE credit
- Self-report on your organization's website
- Keep the email invitation as confirmation for possible future audits
- More info: http://bit.ly/R7CPE

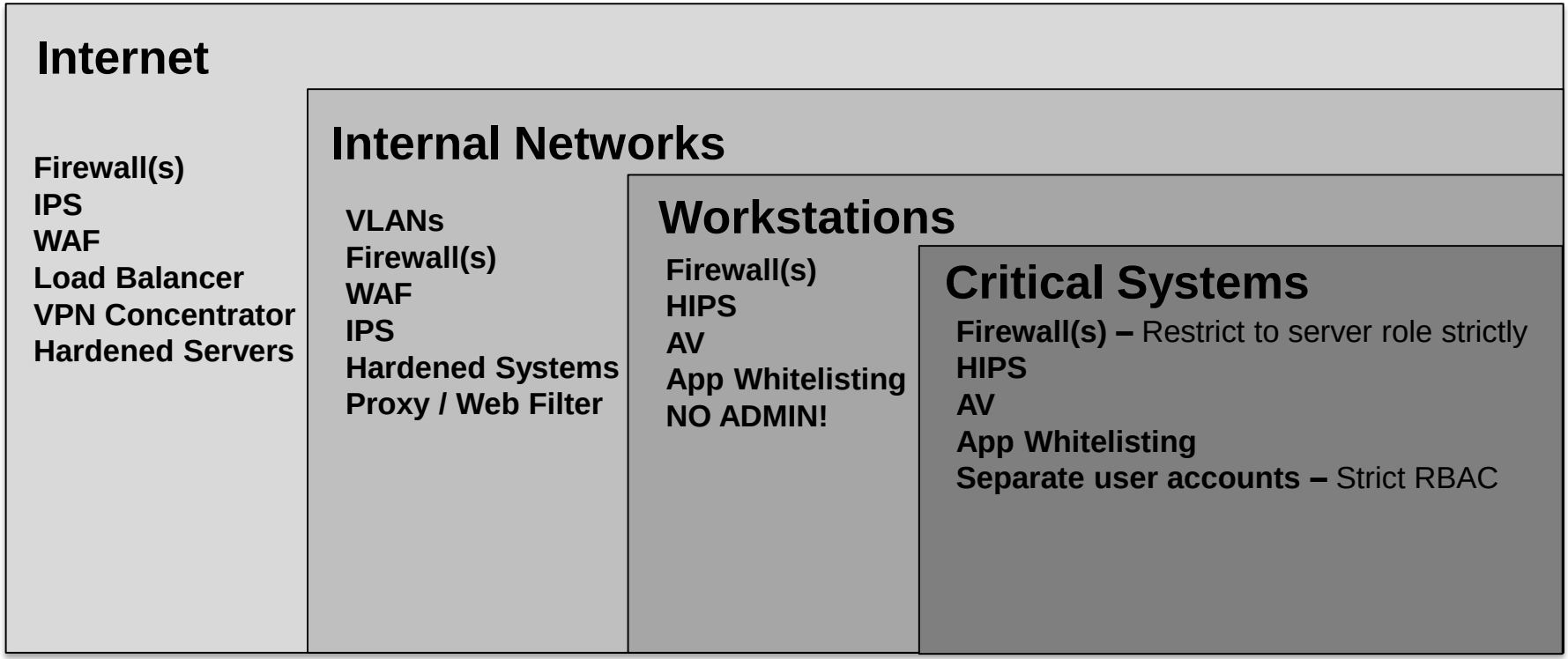
Speakers

Wade Woolwine
Director of IDR Services
Rapid7

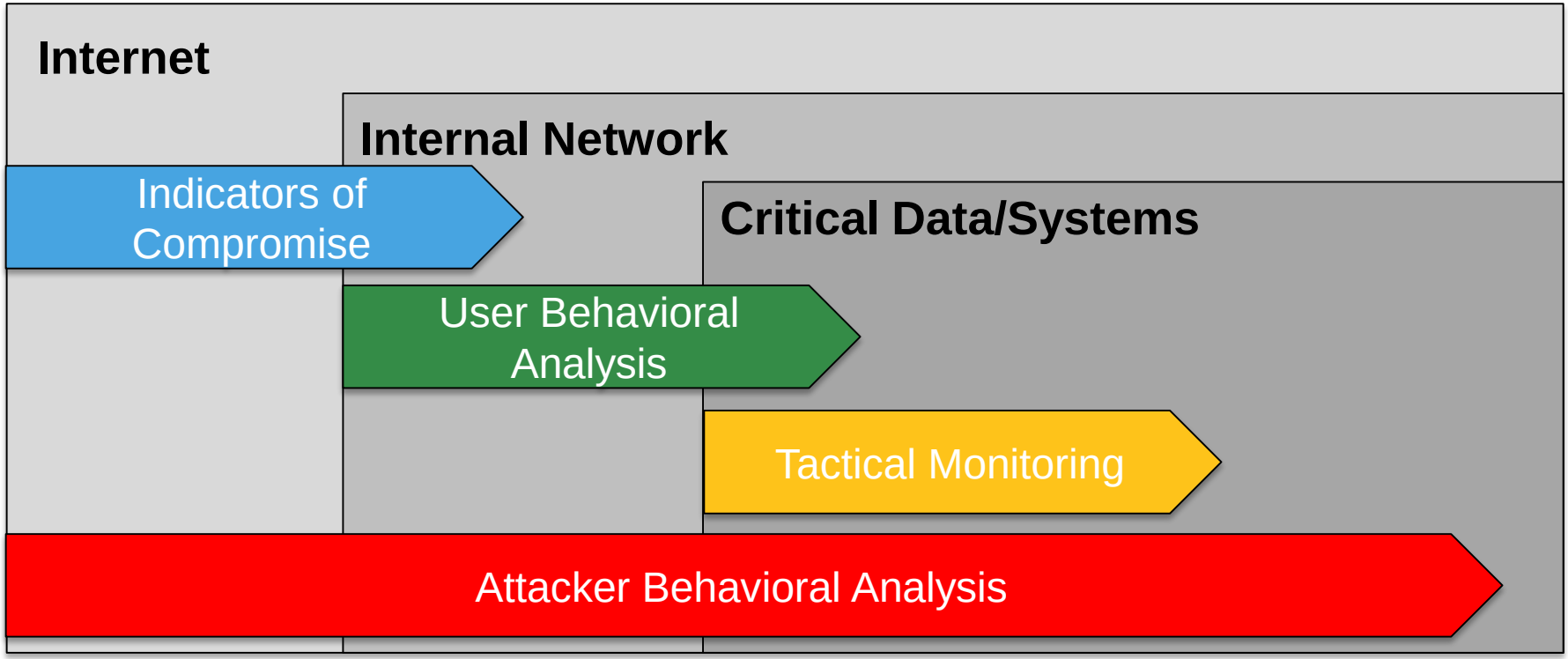
Rebekah Brown
Threat Intelligence Lead
Rapid7

What is Threat Intelligence?

Defense In Depth



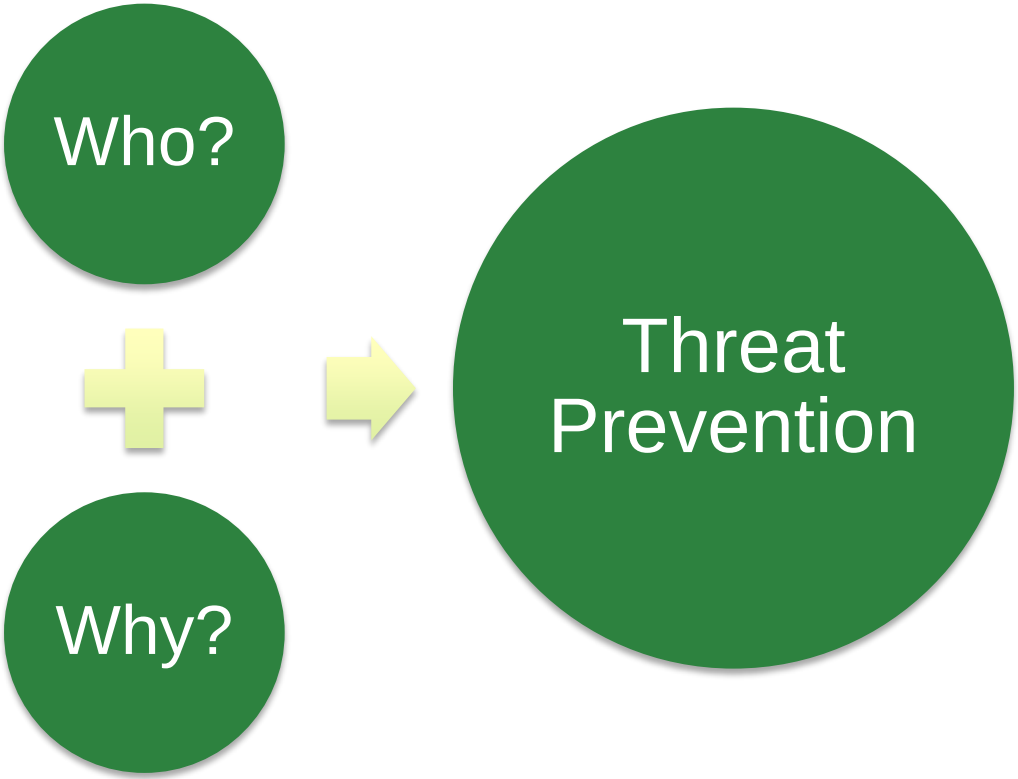
Effective Threat Monitoring



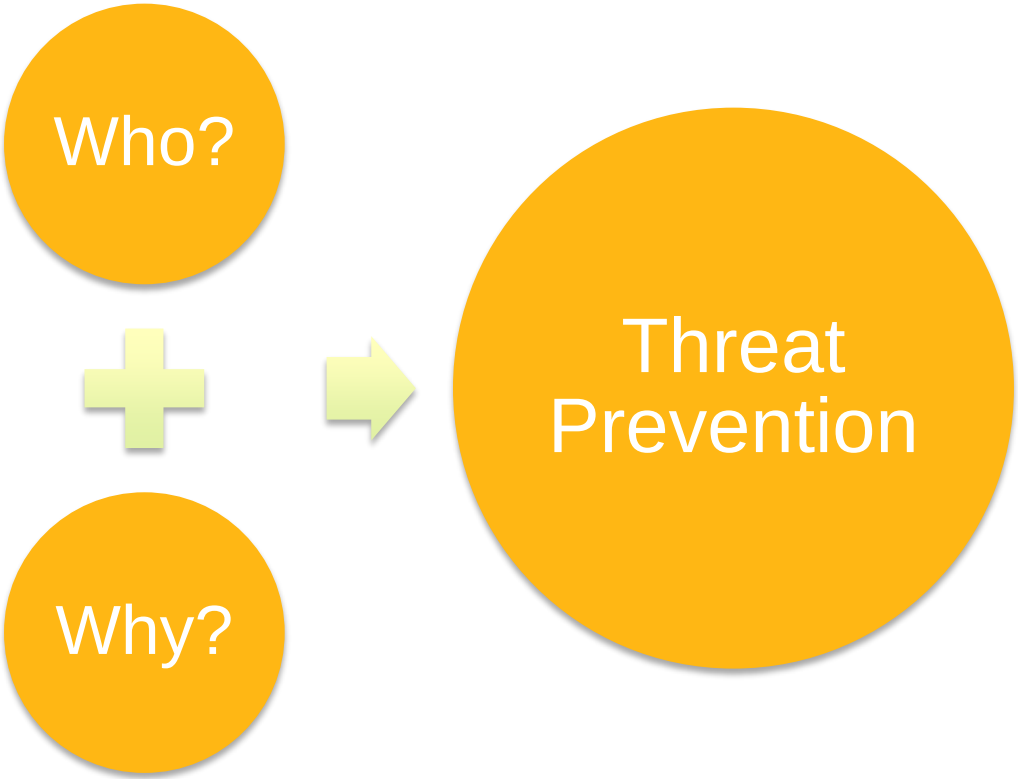
How to Get Started

- What do you have that attackers want?
- Where is that data used and saved?
- What is your attack surface?
- What technology resources do you have?
- What people resources do you have?
- Do you have positive control?

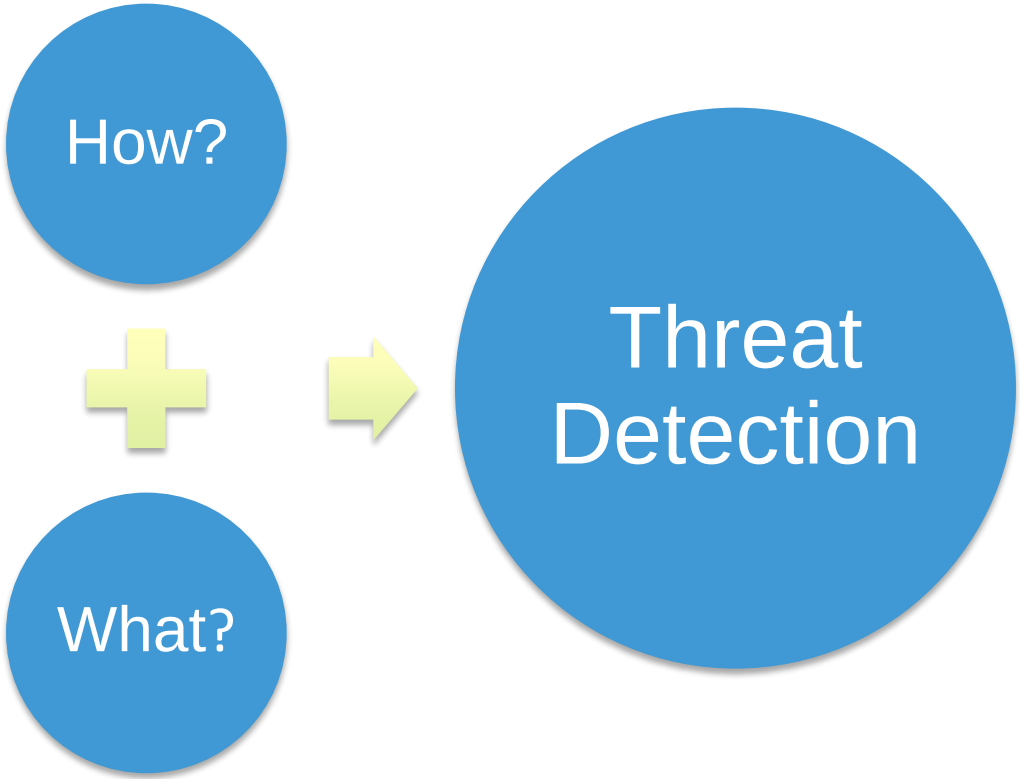
Strategic Intelligence



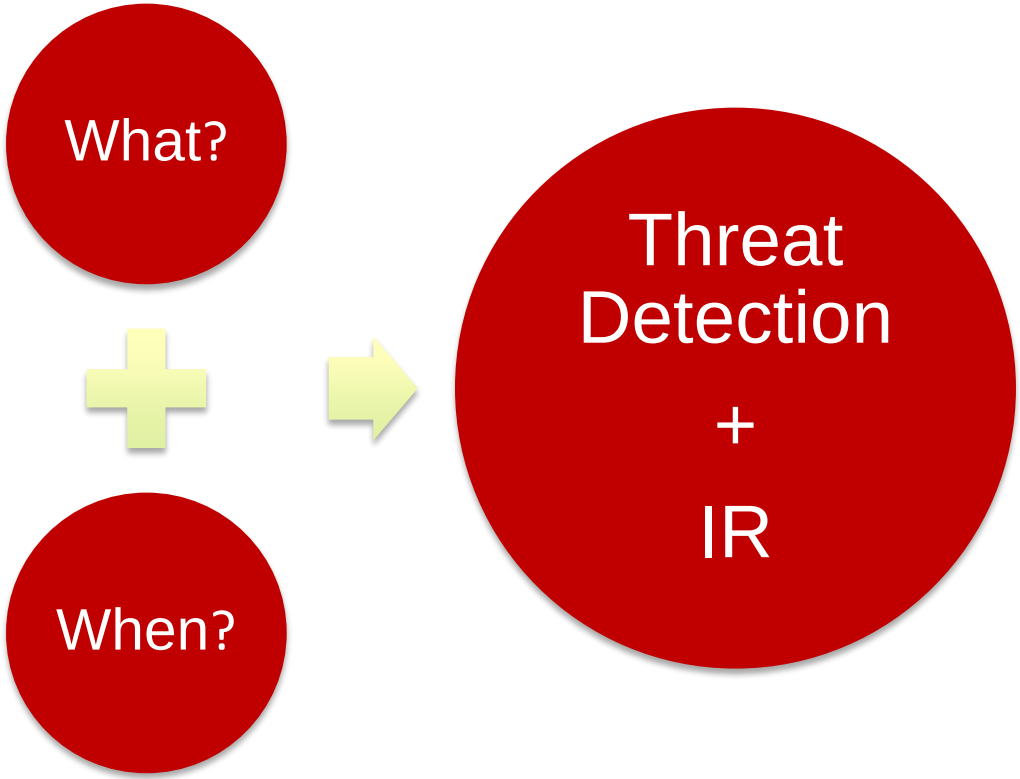
Operational Intelligence



Tactical Intelligence



Technical Intelligence



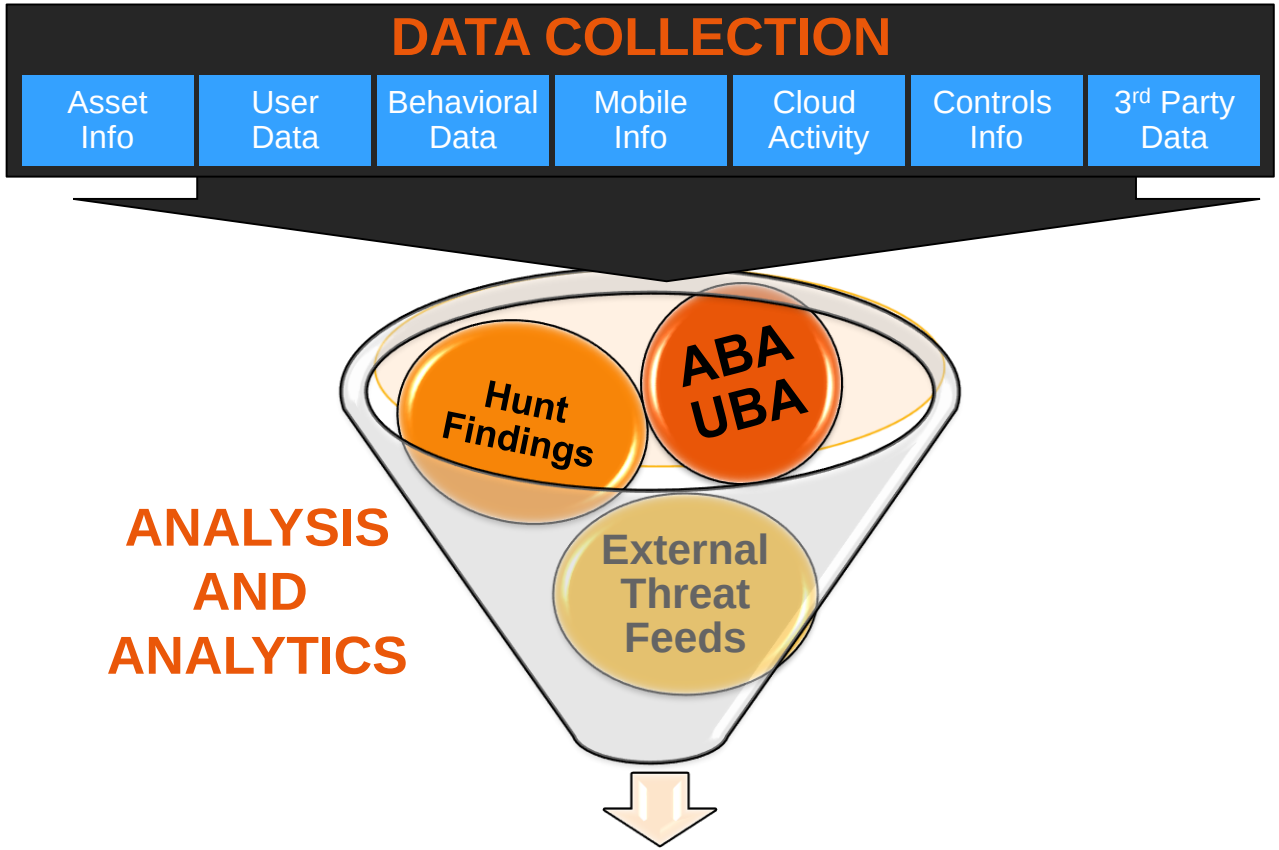
Evaluating Threat Intelligence

- Identify the types of TI offered
- Identify sources
  - Open source threat intelligence
  - Commercial threat intelligence
  - Sharing groups
- Technical Quality Evaluation
- Ease of integration

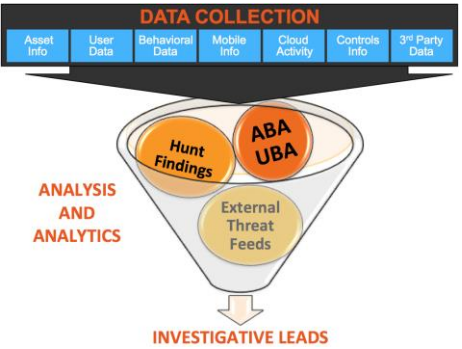
End User Awareness

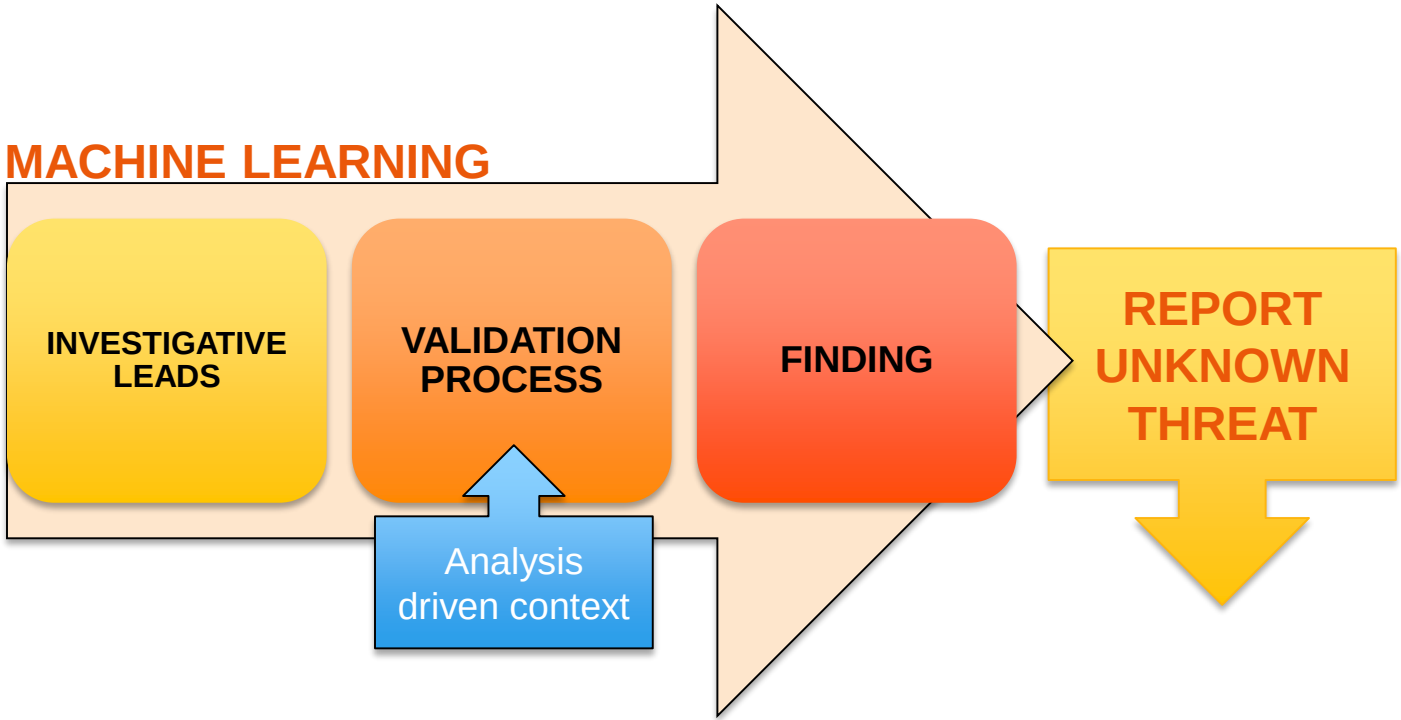
1. Understanding the threat
2. Acknowledge risk
3. Change behavior

Data Analytics to Power Analysts

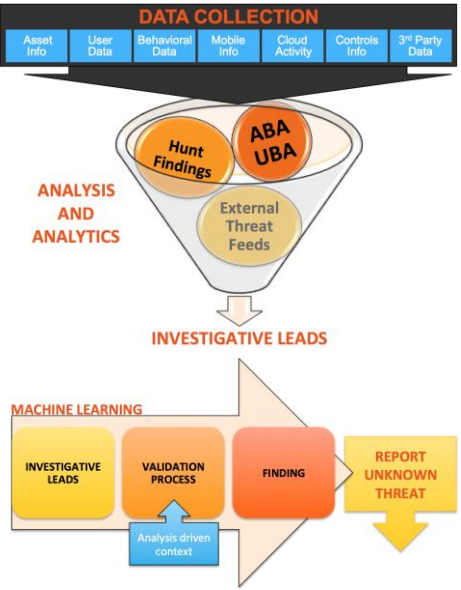


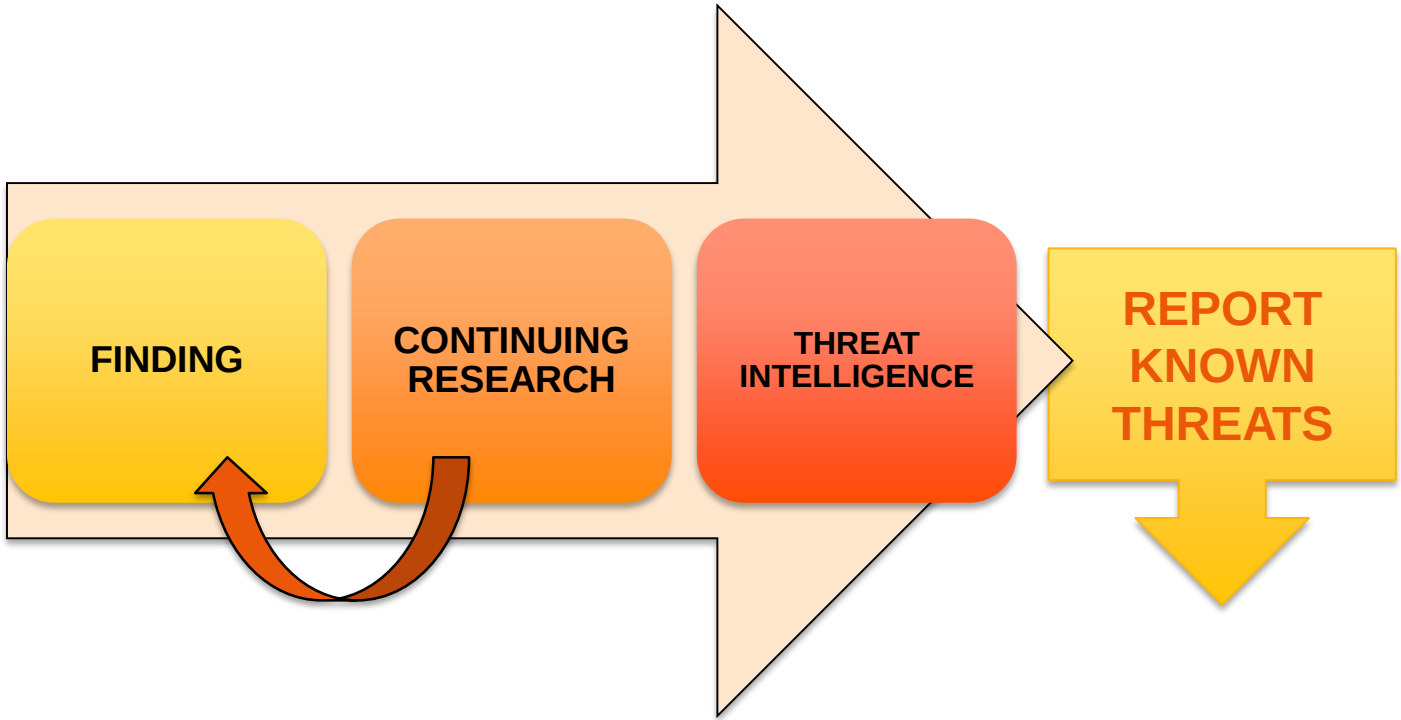
Detecting Unknown Threats





Continuous Detection Improvements





QUESTIONS?

INFO@RAPID7.COM