FORRESTER®

Threat Intelligence to the Rescue?

Rick Holland, Principal Analyst

11 June 2014

@rickhholland

Threat intelligence is flaming hot!!

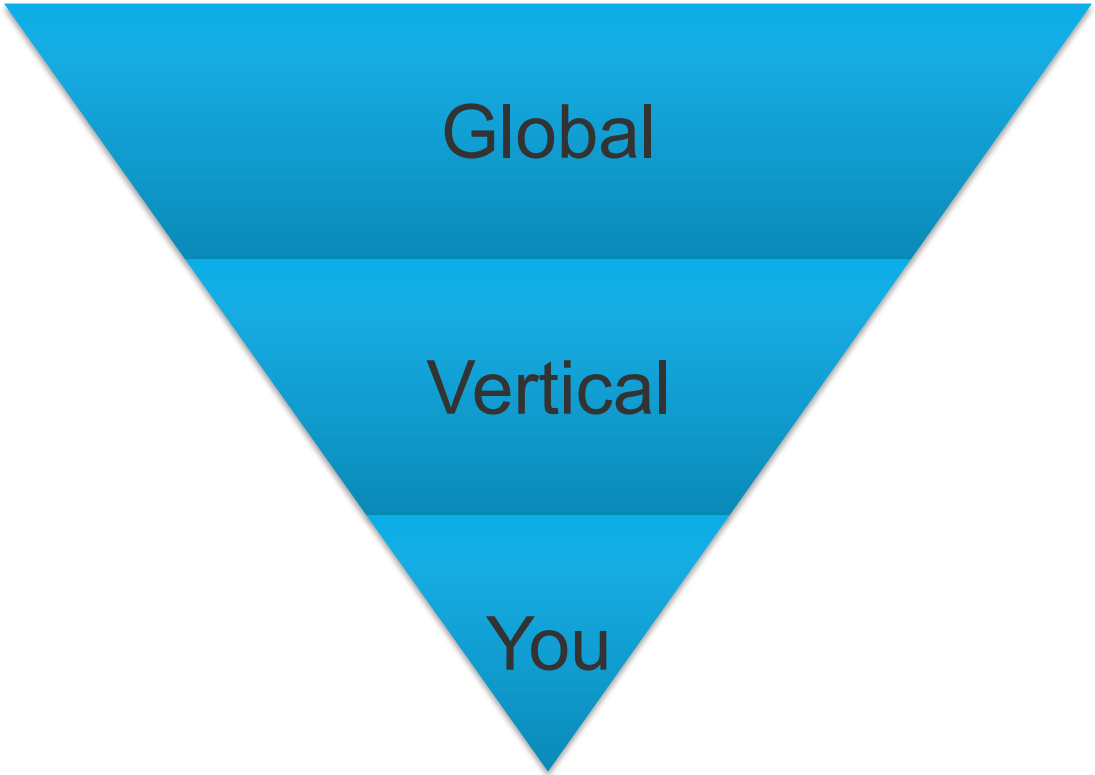
ZERO DARK THIRTY

DOOMSDAY PREPPERS

Actionable intelligence!

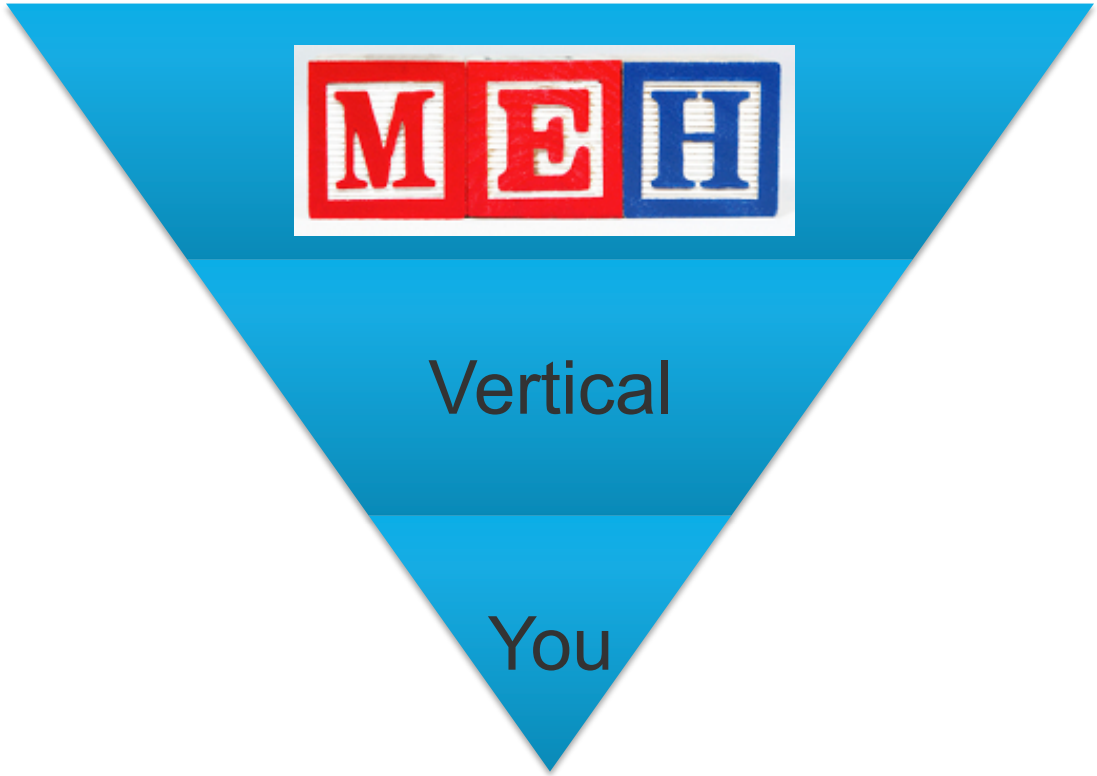
© 2014 Forrester Research, Inc. Reproduction Prohibited

How relevant is the intel to your org?



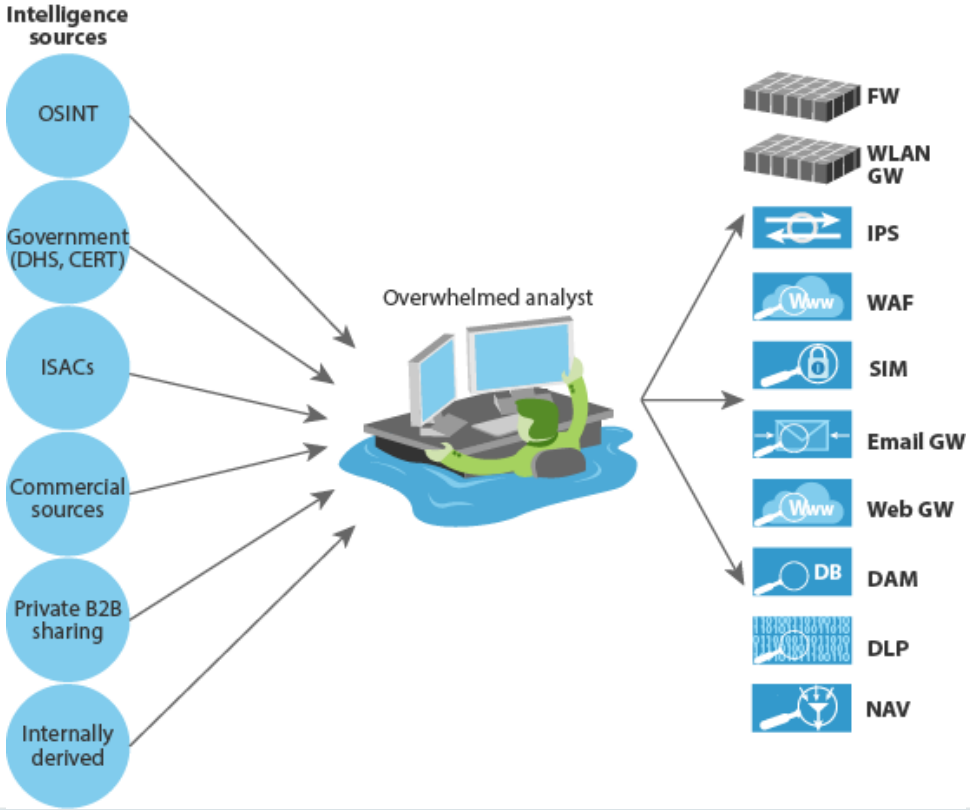
© 2014 Forrester Research, Inc. Reproduction Prohibited

How relevant is the intel to your org?



© 2014 Forrester Research, Inc. Reproduction Prohibited

~~Intelligence~~ Alert driven security



© 2014 Forrester Research, Inc. Reproduction Prohibited

Targeted-Attack Hierarchy of Needs

© 2014 Forrester Research, Inc. Reproduction Prohibited

Strategic threat intel program

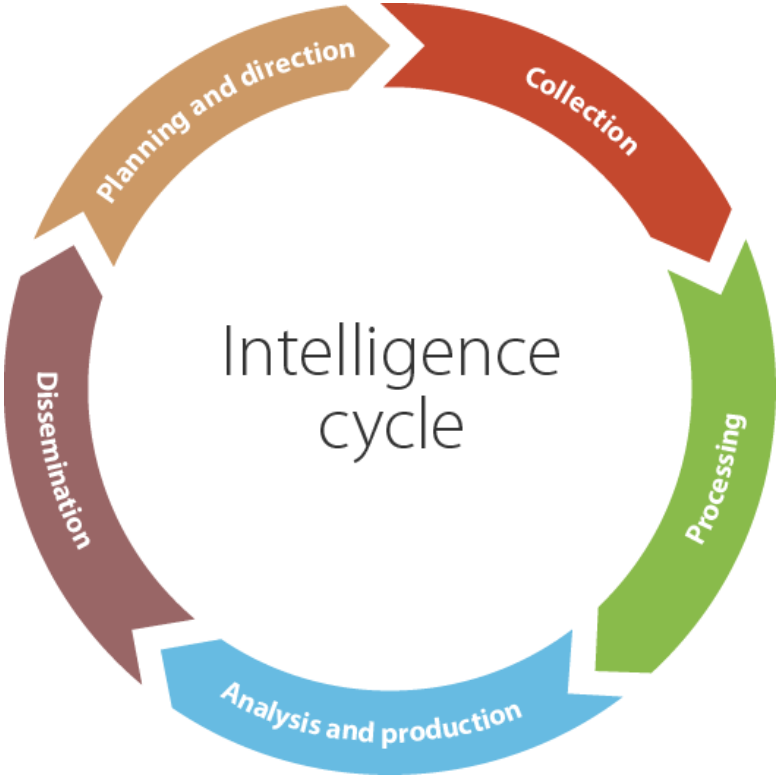
- CISOs want to invest in a strategic program, not in a bunch of feeds.
- What is a strategic TI program?
  - TI doesn't exist for the sake of intelligence; it serves a specific purpose.
  - TI should answer questions about the threat that informs business decisions.

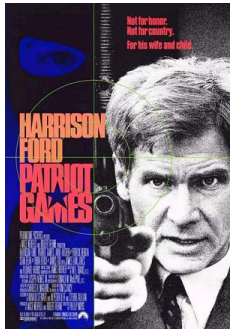
© 2014 Forrester Research, Inc. Reproduction Prohibited

What are you trying
to protect?

What are adversaries targeting?

The Intelligence Cycle





© 2014 Forrester Research, Inc. Reproduction Prohibited

Planning and direction

Developing intelligence requirements	
Establish business relationships	Audit Committee, Business Operations, Risk Management, Legal, Compliance
Understand business success factors	• Build on relationships. • SEC Forms: Annual reports & 10-K • Google Alerts on your organization (e.g., press releases on significant initiatives)
How would an adversary thwart these success factors?	Threat model against the highest priority risks.

© 2014 Forrester Research, Inc. Reproduction Prohibited

You don’t want to have to meet with the Bobs

© 2014 Forrester Research, Inc. Reproduction Prohibited

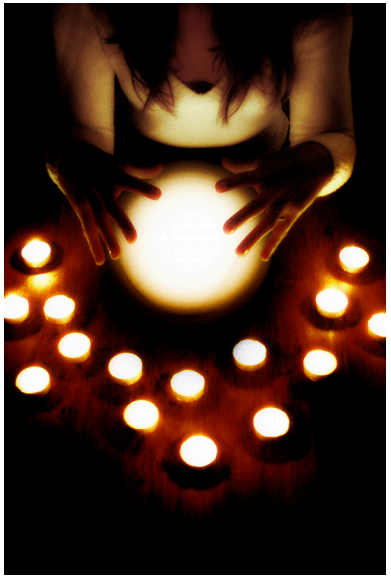
Demonstrate value

- Use TI to show wins. How has the TI program reduced/mitigated risk?
- Measure time to detection/ containment/remediation improvements as a result of TI program.
- Measure “headlines avoided.”

© 2014 Forrester Research, Inc. Reproduction Prohibited

Looking ahead

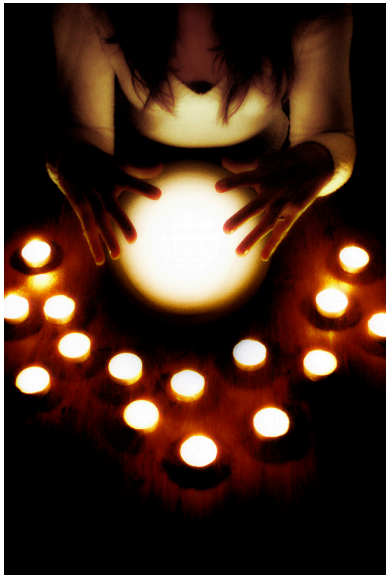
- Commercial offerings are emerging and will mature.
- Sharing will increase; DHS & MITRE enabling this.
- Most orgs will rely upon vendors; don’t have the resources.



© 2014 Forrester Research, Inc. Reproduction Prohibited

Looking ahead

- As enterprises mature their intelligence programs, the adversaries will:
  - Improve their Operational Security (OPSEC)
  - Increase the use of counter-intelligence tactics (e.g., false flags.)



© 2014 Forrester Research, Inc. Reproduction Prohibited

Best definition of APT

© 2014 Forrester Research, Inc. Reproduction Prohibited

Thank you

Rick Holland

+1 469.221.5359

rholland@forrester.com

@rickhholland

forrester.com