Rethinking Threat Intelligence

Danny Pickens, Director, Threat Intelligence
Today’s Agenda

• **Threat Intelligence Market**: 100+ Vendors in play
• **Shifting Domains**: Cold War to Now
• **Intelligence**: Let’s define it
• **The Process**: It is a PROCESS
• **Intelligence Problems**: Remove the F.U.D.?
• **Take-aways**: Seriously… but you should have been taking notes
What CTI Solutions Exist Today?

There are an increasing number of tools, vendors and data in the CTI market.

"Many organization’s legacy processes and technologies are being pushed past intended capabilities...approximately one-third of enterprises studied have bought into the threat intelligence solution space because they believe there is value...yet very few have been able to articulate that value in a meaningful and business-relevant manner." - Optiv Solutions Research
Shifting Domains

Cold War

Counterterrorism

Cyber
“…Our collective ignorance of intelligence has undermined not only our intelligence capabilities, but ultimately the policy makers and citizens served.”

~ Henry A. Crumpton
The Art of Intelligence: Lessons from a Life in the CIA’s Clandestine Service

“[Many] just think you can ‘buy intelligence’ or ‘download intelligence’ and don’t realize they need to ‘develop intelligence’.”

~ Scott Roberts
Director of Bad Guy Catching
GitHub
Intelligence Defined

**Intelligence** is an ecosystem supportive of the decision making process derived from the collection, analysis, dissemination and integration of threats and vulnerabilities to an organization and its people and assets.

**Why Intelligence?**
- Informs and Shapes Policy
- Drives Operations
- Leads Response

**Because Intelligence is:**
- Both a process and a product
- Enhances situational awareness
- KNOWLEDGE
The Process

Dissemination & Integration
Planning & Requirements
Analysis & Production
Collection

Intelligence Cycle
Actor Intention

MICE

- Money
- Ideology
- Compromise
- Ego
Intelligence: F.U.D.

FUD = Feeds Under Duress
Even Batman Needs Intelligence

- ALFRED
  Targeting of Employees

- BAT CAVE
  Facilities / Geo Locations

- THE JOKER
  Adversary

- POLICE
  Competition Third Party

- Gotham
  Case Statistics
The Takeaway

Define what **INTELLIGENCE** is for you

Use the **Process** to build **Products**

Use intelligence to **SHAPE** your program

**EDUCATE** based off of historical data

Move from feed based intelligence to **ANALYSIS**
Questions

Danny Pickens
Director, Threat Intelligence
Optiv MSS
Danny.Pickens@optiv.com
Resources:

• Professional Resources
  – U.S. Army ADRP 2-0: Intelligence
  – Intelligence and National Security Alliance (INSA) Whitepapers

• Books
  – “Psychology of Intelligence Analysis”, Richards Heuer Jr.
  – “Killer Elite”, Michael Smith
  – “Silent Warfare: Understanding the World of Intelligence”, Abarm Shulsky
  – “Open Source Intelligence Techniques – 3rd Edition”, Michael Bazzell